DANYIIL TUROVSZKIJ

# OROSZ HEKKEREK

## ÍGY LETTEK LÁZADÓKBÓL PUTYIN KATONÁI

FORDÍTOTTA GYÜRKY KATALIN

Danyiil Turovszkij

# Orosz hekkerek

*Így lettek lázadókból Putyin katonái*

ATHENAEUM

A fordítás alapjául szolgáló mű:

Даниил Туровский: Вторжение:
Краткая история русских хакеров

© Daniil Turovsky, all rights reserved.

Published by arrangement
with ELKOST Intl. Literary Agency

Hungarian translation © Gyürky Katalin, 2020
Minden jog fenntartva.

Kiadta az Athenaeum Kiadó,
az 1795-ben alapított Magyar Könyvkiadók
és Könyvterjesztők Egyesülésének tagja.
1086 Budapest, Dankó u. 4–8.
Telefon: 1-235-5030
www.athenaeum.hu
www.facebook.com/athenaeumkiado

ISBN 978 963 543 015 4

Felelős kiadó: Dian Viktória
Felelős szerkesztő: Besze Barbara
Szerkesztette: Lakner Zoltán
Szaklektor: Solymos Ákos CISM, CRISC és Zsiros Péter
Műszaki vezető: Drótos Szilvia
Borító: Földi Andrea
Nyomdai előkészítés: Tóth Viktor

Készült a Central Dabasi Nyomda Zrt.-ben, 2020-ban
Felelős vezető: Balizs Attila vezérigazgató

A szüleimnek,
mert kíváncsiságra tanítottak

# Előszó

Az orosz hekkerek története az egykori Szovjetunió kamaszainak története. Szovjet mérnöki családokban nőttek fel, fiatalkorukban kiberpunkot és tudományos-fantasztikus műveket olvastak, a piacokon IBM-utánzat számítógépeket vásároltak, majd egyszer csak hekkerfórumokon találták magukat, amelyek a sokszor lehangoló orosz élet, az ablakukból látszó koszos utcák, az üresség és a kilátástalan jövőtől való félelem helyett a kiutat jelentették a számukra.

Amikor az Egyesült Államokban az úgynevezett dotcomok gazdasági lufija kezdett nagyra nőni, Oroszországban a hekkerek beindították aranyüzletüket: az amerikai hitelkártya-adatok ellopása, a bankszámlák és a webshopok feltörése sok millió dollárt hozott. Egyesek – a rablóktól vagy az államtól tartva – gondosan elrejtették ezeket a milliókat, virágüzletekbe vagy gumiabroncs-szerelő műhelyekbe fektettek, mások ingatlanokat, drága sportkocsikat vásároltak, megint mások külföldi házakban rendezkedtek be, és oda utaztak, ahol a színek élénkebbek, mint amilyenekhez az ablakon kinézve hozzászoktak: a Maldív-szigetekre, Ciprusra, Izraelbe.

Az ő életrajzuk gyakran az akcióhősökéhez hasonlít. Amikor a múltjukról faggattam őket, úgy tűnt, nem csupán a pénzért csinálták a kétes üzelmeiket, hanem azért, mert könyvek vagy filmek hőseivé szerettek volna válni, azokhoz hasonlókká, akiket annyira szerettek gyerekkorukban.

Fiatalkoromban gyakran olvastam a *Hekker* magazint, amelyből rendszeresen tájékozódhattam, hogyan törjek

fel valamit. Olyan családban nőttem fel, ahol mindenkinek volt számítógépe, boldogan programoztunk, esténként weboldalak kódjait tanulmányoztuk, és megpróbáltuk feltörni azokat. Tizenöt évesen azon gondolkodtam, hogy suli után információbiztonsági karra megyek tanulni, azután pedig, ha lehet, az FSZB-nél* fogok dolgozni. Szerencsére ezek az elképzeléseim elég hamar szertefoszlottak, nemsokára komolyan rajongani kezdtem a szövegek, a történetek és az újságírás iránt.

Mindazonáltal a félig titkos hekkertársadalom, amelybe nem sikerült bekerülnöm, időről időre hallatott magáról. Az elején ismerőseim közösségi oldalait törték fel, és pénzt követeltek tőlük. Később az Oroszországban végzett riporterkedésem miatt az én fiókjaimat támadták meg az állambarát hekkerek.

Ez a könyv a választási lehetőségekről szól, és azokról az utakról, amelyekre azok léptek, akik aztán a hekkerszubkultúra részévé váltak. Míg egyesek megmaradtak romantikusnak, s nem foglalkoztak a pénzzel *(I. rész)*, addig mások meggazdagodtak *(II. rész)*, s amikor eljött az idő, hogy kapcsolatba lépjenek vele, vagy az államnak kezdtek el dolgozni, vagy ellene *(III. és IV. rész)*.

A könyv főként azokból a szövegekből áll össze, amelyeket az utóbbi években a meglehetősen kevés független portálok egyikének, a *Meduzá*nak (meduza.io) írtam, de nem csak erre korlátozódik. Az anyag nagy részét a munkaidőmön túl gyűjtöttem, fórumokat, internetes archívumokat, könyveket búj tam, hekkerekkel találkoztam, kódolt chatszobákban társalogtam velük. Ezeket az embereket orosz hekkereknek nevezem, mert az orosz nyelvű hekkertársadalom egységes maradt: oroszok, ukránok, belaruszok és a volt Szovjetunió egyéb utódállamaiból származók mind ugyanazokon a fórumokon nőttek fel, közös csoportokat alakítottak, és együtt hajtották végre célpontjaik feltörését, még akkor is, amikor az államaik már egymás ellen harcoltak.

Ez a könyv részben útikalauzként szolgál az orosz hekkerek világához – a Szovjetunió utolsó éveitől napjainkig. Részben egyfajta tablókép, részben pedig annak látlelete, hogy az orosz hatóságok hogyan építették fel a világ egyik legharcképesebb kiberhadseregét. A könyvben felvázolt sok-sok, egymástól független emberi történet alapján képet alkothatunk arról, hogy milyen körülmények között nőttek fel a hekkerek, és milyen tényezők határozták meg további sorsukat.

Végeredményben ez a könyv arról szól, hogy számítógép előtt ülő ismeretlenek hogyan képesek konfliktust szítani országok között, hogyan tudják tönkretenni a kritikus infrastruktúrát (például kikapcsolni az áramszolgáltatást akár teljes régiókban), és hogyan képesek ölni úgy, hogy nem hajtanak végre semmiféle hadműveletet, és nem is ismerik az áldozataikat.

* Az FSZB az orosz Szövetségi Biztonsági Szolgálat, a KGB utódszervezete. – *A szerk.*

*Prológus*

# A kiberháború első menekültje

2015. augusztus 22-én szakállas, szemüveges férfi lépett a moszkvai Leningrád vasútállomás épületébe, kezében egy-egy útitáskával. A kasszánál jegyet váltott a legelső Szapszan expresszvonatra, amely négy óra alatt ér Szentpétervárra.

Szentpéterváron a férfi a vasútállomástól nem messze álló mikrobuszhoz sietett. Pétervárott nőtt fel, tudta, hogy a Helsinkiig közlekedő mikrobusz a legolcsóbb és legészrevétlenebb módja, hogy Oroszországból Európába jusson. A jegy nyolcszáz rubelbe kerül, az út nyolc órát vesz igénybe, amit majd egyetemi hallgatók, illetve csempészek társaságában tölt el, akik Oroszországból Finnországba cigarettát, visszafelé pedig háztartási vegyszereket szállítanak.

Pár óra múlva a férfi átkelt a finn határon, és végre kicsit fellélegezhetett. Terve sikerült: lerázta üldözőit. Mindent tökéletesen végiggondolt, nem utazott repülőn, mert akkor biztosan feltartóztatták volna az útlevélvizsgálatnál, vonatjegyét sem az interneten, hanem közvetlenül az állomás pénztárában vette meg. Visszaemlékezett korábbi, az addig megszokott életéből való menekülésére: tíz évvel azelőtt a pétervári trolibuszon, a vasútállomásnál elhaladva döntötte el, hogy átköltözik Moszkvába a barátnőjéhez. Leszállt a következő megállónál, jegyet váltott a vonatra, és elutazott. A barátnőjével később össze is házasodtak.

Helsinkiben a férfi elcsípte a Stockholmba tartó kompot, Svédországban pedig a helyi jogvédőkhöz fordult, hogy a segítségüket kérje a politikai menedékjog kérelmezésében.



Ők visszaküldték Finnországba, ugyanis az európai szabályozás szerint menedéket kérni csak abban az országban lehet, amelyen keresztül az ember beutazott az Európai Unióba.

Miután visszatért Helsinkibe, a szakállas férfi talált egy wifivel rendelkező helyet, és levelet írt munkahelyem, a *Meduza* közös szerkesztőségi e-mail-címére. Az ő e-mail-címében egy orosz kifejezés szerepelt: Mertvajaruka1984. Ez egyszerre utalt George Orwell antiutópiájára és a Perimetr (magyarul: holt kéz) rendszerre, azaz arra a nukleárisfegyverzet-irányítási szisztémára, amelyet a Szovjetunióban a hidegháború tetőpontján hoztak létre. Amerikában *Dead Hand*nek nevezik ezt a rendszert, amelyet állítólag úgy dolgoztak ki, hogy még akkor is ledobja az atombombát, ha mindenki, aki ezt végre tudta volna hajtani, már halott.

A férfi a levélben Alekszandr Vjarjaként mutatkozott be, a Qrator Labs egyik vezetőjeként. Az orosz cég DDoS-támadások* elleni védelemmel foglalkozik. A férfi közölte, hogy az orosz hivatalnokok és a titkosszolgálatok érdeklődnek ez iránt a kiberfegyver iránt, és ő maga tanúja volt annak, hogyan alkalmazzák ezt állami utasításra.

*„Most, amikor az Oroszországi Föderációban a helyzet egyre forrósodik, attól tartok, rá akarnak kényszeríteni arra, hogy támadások megszervezésével foglalkozzam, mivel alkalmas lehetnék a feladatra; ezért úgy döntöttem, hogy tájékoztatom a közvéleményt* – írta Vjarja. – *Úgy vélem, az állampolgároknak tudniuk kell, hogy mire költik a pénzüket ebben a krízishelyzetben. És hogy KI foglalkozik ezekkel a mocskos ügyekkel. Ezek nem kispályás tolvajok. Hogyha korábban mindenki csak találgatott, most már bizonyítékaink vannak ☺ Ha váratlanul el nem üt egy autó, akkor sikerült elhagynom az országot. Ezt a döntést egyáltalán nem volt könnyű meghoznom: elvesztettem egy jó állást, és a családomtól tulajdonképpen a semmibe tá-*

* Lásd a *Fogalomtár*ban.

*voztam. Plusz most az összes cafka, mint amilyen a* Lifenews, *engem fog »bemártani«."*

Azt válaszoltam, szeretném részletesebben megismerni a történetét, és találkozzunk személyesen. Beszélgetésünk rögvest átkerült a Telegram* titkos chatszobájába: 2015 Oroszországában tömegesen használták a védett csetelést, miután rájöttek, hogy az orosz titkosszolgálatok le tudják hallgatni és el tudják olvasni a nyitott csatornákat, habár a törvény szerint ehhez először bírósági engedélyt kell kapniuk.

*– Milyen gyorsan tudna ideutazni? Arra készültem, hogy megyek, feladom magam, és védelmet kérek* – írta Vjarja.

*– Holnapután?*

*– Ó.*

*– Az késő?*

*– Először is valahol meg kell szállnom.*

*– Megpróbálhatom holnap is.*

*– Ó, igyekszem találni valami hotelt, már csak négy egység maradt a kártyámon.*

Vjarja az egyik városi hostel sokágyas szobájában szállt meg. Helsinki drága város, de szerencséje volt, és talált napi húsz euróért szállást. Másnap reggel, amikor felültem a repülőgépre, ezt az üzenetet kaptam tőle: *„Szavakkal ki sem fejezhető tapasztalat a hostel. Horkolnak, álmukban beszélnek, és lopnak egész éjszaka."*

Hamarosan egy folyóparthoz közeli plázában találkoztunk. Vjarja a bejáratnál állt, miközben idegesen forgolódott, és engem figyelt a villamossíneken átvágó emberek között. Az összes holmija – a két útitáskája – nála volt. Bementünk a legközelebbi kávézóba, megrendeltük a kávét, ő pedig mesélni kezdett.

* * *

* A Telegram Oroszországban népszerű üzenetküldő alkalmazás. – *A szerk.*



Alekszandr Vjarja az 1980-as évek közepén született egy leningrádi kommunalkában,* és apa nélkül nőtt fel. Tizenkét éves volt, amikor rajongani kezdett a számítógépekért – először a videójátékokért, aztán a programozásért és a „vasért", azaz a számítógépért. Az első munkahelye az anyja unokatestvérénél volt, egy rendszergazdai állás. A közösségi oldalak akkor még épp csak megjelentek, de Vjarjának ezeken elvből nem voltak fiókjai: nem akart semmiféle nyomot hagyni maga után az interneten.

Miután átköltözött Moszkvába, hálózati mérnökként dolgozott különböző webtárhely-szolgáltatóknál. 2012-ben talált az egyik erre szakosodott fórumon egy érdekesnek tűnő, megüresedett állást, és néhány tesztfeladat után felvették a Qrator Társasághoz, amely a DDoS-támadások elleni védelemre specializálódott.

Ekkorra a cég már piacvezetőnek számított, kliensei közül többen is az orosz média független szereplői közül kerültek ki, mint a Dozsgy tévécsatorna, a *Novaja Gazeta* és a *Vedomosztyi* újságok, ezenkívül ügyfelei voltak bankok (az Alfa és a Tyinykoff) és internetes áruházak (Julmart, Lamoda). Vjarja szerint az általa nyújtott szolgáltatásokat egyszer még egy cédrushordókkal kereskedő internetes webáruház is igénybe vette, de nincs is ezen mit csodálkozni, hiszen épp e webáruház ellen hajtották végre a legkomolyabb támadást azalatt, amíg ő a társaságnál dolgozott. Oroszországban népszerű módja a konkurenciával való leszámolásnak a DDoS-támadás, van olyan üzlet, amelyik egyetlen nap leforgása alatt kényszerül bezárni – magyarázta. Az ilyen támadások nem kerülnek sokba (körülbelül napi háromezer rubelbe), és ennek révén ki tudják vonni

* A kommunalka a szovjet időkre jellemző lakóhelyféleség, társbérlet: egy nagyobb lakást kisebb részekre osztottak annak érdekében, hogy minél több családnak legyen hol laknia. Az ilyen épületekben azonban a konyha és a mellékhelyiség közös használatú volt. – *A fordító megjegyzése.*

a védelem nélküli weboldalt a rendszerből, ami az adott cégnek komoly veszteséget okoz.

Vjarja a műszaki vevőszolgálatnál dolgozott, és a kliensek folyamatosan bejövő telefonhívásait kezelte. Gyakori volt, hogy a Qratorhoz olyanok fordultak, akik azért voltak elégedetlenek, mert a cég többek között a velük ellenséges weboldalakat is védte. 2012 tavaszán – Vlagyimir Putyin elnöki beiktatásának előestéjén – állambarát patrióta hekkerek megtámadták az *Ekho Moszkvi*, a *Kommerszant* és a Dozsgy weboldalait – ezek mindannyian a Qrator kliensei voltak. „Hát maguk miért védik a zsidókat?" – kérdezte Vjarjától az egyik aznapi betelefonáló.

A 2013-as moszkvai polgármester-választás idején a Qrator védte Alekszej Navalnij weboldalát; az ellenzéki politikus jelöltette magát, és sikeres kampányt folytatott. Vjarja egyszer észrevett egy lesötétített ablakú furgont az irodájuk mellett, a tetején antennákkal. A következő napokban a furgon szinte mindennap megjelent. Amikor kimentek ebédelni, a Qrator munkatársai megpróbáltak benézni a kocsiba, és azon tréfálkoztak, hogy fánkot kéne hozni annak, aki lehallgatja őket.

„– Szása tehetséges ember, de nagyon érzékeny és bogaras – mesélte Vjarja egykori főnöke, Alekszandr Ljamin. – Ha túl sokáig dolgozol az informatikai védelem területén, kezdesz megváltozni, kezdesz mindenben fenyegetést látni."

Bárhogy is álljon a dolog, 2015-re Vjarja ennél a cégnél az üzemeltetési vezető pozícióig vitte. Mind gyakrabban utazott külföldre. Azért kellett európai adatközpontokat látogatnia, hogy olyan szoftvereket telepítsen, amelyek magas leterheltség, például támadások esetén is működőképesek. A Qratorban az ilyen szervereket „az információáramlás tisztító központjainak" nevezik. Ezek segítik az ügyfelek honlapjait virtuális határvédelemmel és forgalomelemző programokkal körbevenni, amik kiszűrik a káros információ áradatot az ártalmatlanból. Ugyanebben az időben a cég megkezdte az előkészületeket, hogy megnyissa az első külföldi részlegét Prágában. Minden munkatárs dolgozói vízumot kapott. A fiókintézet vezetésével Vjarját bízták meg.

2015. február 3-án a Qrator főigazgatóját, Alekszandr Ljamint felhívta Vartan Hacsaturov, a Minkomvszjaz infrastrukturális projektek ügyosztályának helyettes vezetője. Hacsaturov olyasvalakit kért a társaság munkatársai közül, aki segítene tisztviselőinek az egyik „kényes kérdésben". Vjarján kívül nem volt más, a többiek szétszéledtek a világban különböző konferenciákra.

Hacsaturov kapcsolatba lépett Vjarjával, és meghagyta a telefonszámát, amire Vjarja üzenetet küldhetett. Kora este megszólalt a telefon. Egy bizonyos Vaszilij Brovko telefonált. Vjarjának fogalma sem volt róla, hogy kicsoda ő. Brovko azt mondta neki, néhány nap múlva feltétlenül el kell repülniük együtt Szófiába, az asszisztensnője az összes ehhez szükséges dokumentumot előkészíti.

Vjarja rákeresett Brovkóra az interneten, és a fejéhez kapott. Leginkább az ütött szöget a fejébe, hogy Brovko alapította az Apostol nevű céget, amelyet 2013 tavaszán Alekszej Navalnij azzal vádolt, hogy botok segítségével behatolt az Aeroflot légitársaság közösségi oldalára. Az utóbbi időben Brovko a Rosztech kommunikációs ügyosztályának vezetőjeként dolgozott, annál az állami konszernnél, ahol állami és katonai megrendelésre állítottak elő modern technológiát képviselő termékeket. A Rosztechet Szergej Csemezov, Vlagyimir Putyin közeli ismerőse vezette.

Vjarja azt feltételezte, hogy Brovko majd az ő szakmájába vágó segítséget kér tőle, vagyis hogy fejlessze ki a DDoS-támadások elleni védelem új rendszerét. És érdekes módon éppen akkor hívták Bulgáriába, amikor a hasonló védelmi programok kidolgozásáról ismert munkatársak mind Izraelben vagy az Egyesült Államokban tartózkodtak.

2015. február 5-én Vjarja elrepült Szófiába. Küldött egy üzenetet Brovkónak, akitől az a válasz érkezett, hogy a találkozójuk csak délután fog összejönni. Vjarja sétálgatott a belvárosban, aztán odament a kijelölt helyre, a pompázatos Grand Hotel Sofia üvegépületéhez.

Brovko. Az egyik kezében orosz gyártmányú okostelefon, a másikban egy iPhone volt, és folyton valamelyiket nyomogatta. Vjarja, miután üdvözölte Brovkót, azt mondta neki, hogy Szófia csodálatos kis város. „Szemétgödör" – vetette oda válaszul Brovko.

Brovko nyomában megjelent két férfi. Úgy mutatkoztak be mint a helyi Packet Technologies társaság munkatársai (a társaság weboldala[1] szerényen közli, hogy a szervezet a fejlett hálózati technológiák tervezésére szakosodott). Brovko azt mondta Vjarjának, hogy muszáj bemenniük a társaság irodájába „megszemlélni a terméket," és elmondaniuk róla a véleményüket.

Az iroda nem volt messze. A Packet Technologies egyik képviselője elkezdte a prezentációt, de közben magáról beszélt: az izraeli hadseregnél szolgált, ahol a legnagyobb internetes cégek tanácsadójaként dolgozott hálózati védelemmel kapcsolatban, és hogy részt vett a *Black Hat*en (ez a világ legfontosabb információbiztonsági konferenciája, amelyre az IT-társaságok képviselői és a hekkerek is el szoktak utazni).

Ezt követően a bolgár cég munkatársa, Vjarja állítása szerint, kijelentette: „Most pedig egy DDoS-támadás megszervezésére szolgáló terméket fogok ajánlani önnek." A programnak nem volt neve.

A munkatárs hozzátette, hogy a „termék" képes a DDoS-támadást hálózati szinten megszervezni. Az ilyen támadások káros adatcsomagokkal „dugítják el" a szerver erőforrásait, így az képtelen a hasznos adatforgalom lebonyolítására.

A rendszer egy kis készülék volt, egy „doboz", hozzá tartozó szoftverrel, amelyet egy adatcsereközponton telepítettek. A „termék" részére egy maximálisan 10 gigabit/



másodperc adatsebességű sávot különítettek el. A Packet Technologies munkatársai hozzátették, hogy a rendszer képes „koktélszerű", tehát kevert, a legnehezebben elhárítható típusú támadás végrehajtására is. Ezenkívül egy újabb „doboz" beiktatásával könnyen növelhető az adatforgalom sebessége. 2010-ben, a Wikileaks szervereit 10 gigabit/másodperc erősségű támadás érte. Az internet történetének legnagyobb DDoS-támadását[2] a holland Cyberbunker nevű tárhelyszolgáltató követte el a Spamhaus szervezet ellen, erőssége 300 gigabit/másodperc volt. A *The New York Times* írása szerint „lelassította az internetet".

Amikor az elméleti résszel végzett, a társaság munkatársa VPN-kapcsolaton keresztül nyitotta meg a Tor böngészőt, így biztosított anonimitást saját maga számára (az így indított támadás nyomon követése szinte lehetetlen). Az IP-cím begépelése után egy roppant egyszerű felületű honlap jelent meg. Fent a címsor, lejjebb a DDoS-támadás tíz altípusa jelent meg, mindegyik mellett üres, kipipálható rubrikával. Lent egy gomb volt látható, amellyel a támadás erősségét lehetett beállítani, 100 megabit/másodperctől 10 gigabit/másodpercig. „Nem szükséges teljesen feltekerni, ha az áldozat nem túl nagy" – magyarázza Vjarja.

A cég munkatársai a felületen beírták az ukrán védelmi minisztérium weboldalának címét. A szomszédos ablakban megnyitották a szolgáltatásoldalt, aminek alapján meg lehetett állapítani a weboldalak kapacitását. Majd bekapcsolták a programot. Megjelent a támadás erősségét mutató grafikon, amely hamar elérte a 10 gigabit/másodpercet. A kapacitásszolgáltatás azt mutatta, hogy a weboldal nem elérhető. Megpróbálták megnyitni a böngészőn, de ott sem volt elérhető. Néhány perc múlva a támadás leállt, és a weboldalt ismét meg lehetett nyitni.

Majd megpróbálták az ukrán védelmi minisztérium weboldalát 100 megabit/másodperc erősséggel támadni, és az ismét működésképtelenné vált.

„Végezzünk egy felülvizsgálatot a slon.ru-n" – ajánlotta Brovko, aki eddig hallgatott (párbeszédjüket Vjarja szavai alapján reprodukálom). A Szlon* (most így hívják a Republicot) az egyik legnépszerűbb független hírszolgáltató Oroszországban, amelyet 10 gigabit/másodperc erősséggel támadtak meg. A weboldalt nem lehetett megnyitni, és néhány percig elérhetetlen volt. Később a Szlon akkori főszerkesztője, Makszim Kasulinszkij visszaigazolta nekem, hogy 2015. február 5-én észleltek egy támadást, amely két percig bedöntötte a weboldalukat.

„És mi van akkor, ha a weboldalak védelmet használnak? Feltörik őket?" – kérdezte Vjarja. Azt a választ kapta, hogy ebben az esetben kénytelenek megtudni a szerver valódi címét (minden védelmi szolgáltatás átereszti magán a támadást, de a szerver valódi címét álcázzák), és a Packet Technologiesnél van egy erre kidolgozott eljárás. Vjarja tisztázni akarta, mennyibe kerül a rendszer, amire Brovko, Vjarja elmondása szerint, ezt válaszolta: „Körülbelül egymillió dollár."

A találkozás után Vjarja és Brovko a Grand Hotel Sofiába indult. Beültek az előcsarnokba kávézni. Vjarja úgy emlékszik, Brovkót az érdekelte mindennél jobban, hogyan lehet megtalálni a weboldal valódi címét, és melyik információcserét biztosító rendszerre a legjobb ráállítani egy ilyen programot. Egy kis idő múlva a Rosztech munkatársa állítólag ezt mondta: „Nos, nekünk szükségünk van valakire, aki ezt irányítani fogja." Vjarja félrenyelt, és ezt mondta: „Nem, ne haragudjon. Én nem vagyok hekker. Ez ellenkezik az elveimmel, és törvényellenes." Brovko, Vjarja szavai alapján, ezt kérdezte: „Tisztában vagy vele, hogy milyen szervezet küldött ide téged?" Vjarja magában azt feltételezte, hogy Brovko az FSZB-re utal, de csak annyit

* A *szlon* szó oroszul elefántot jelent, utalva a hírszolgáltató gigantikus méretére. – *A fordító megjegyzése.*



mondott, hogy ezentúl kizárólag a műszaki részleg bevonásával hajlandó válaszolni a kérdésekre. Bejelölték egymást Telegramon, és ki-ki ment a maga útjára.

Elmondása szerint Vjarját sokkolták a történtek. Rögtön megírt mindent a főnökének, Ljaminnak, aki azt tanácsolta, hogy „maximálisan tartsa magát ettől távol". Másnap, február 6-án, Vjarja visszatért Moszkvába.

Vjarja rendelkezésemre bocsátotta a Brovkóval és a saját feletteseivel folytatott további levelezéséről készített képernyőképeket. A Rosztech munkatársát néhány üzenetben technikai tanácsokkal látta el. Elsősorban azt ajánlotta, használjanak holland adatcsereközpontokat, ahol a sok terrabit adatforgalom mellett a néhány tucat gigabit fel sem tűnik. Brovko röviden válaszolt: „Köszönöm. Megvizsgálom."

2015. március 5-én Brovko asszisztensnője írt Vjarjának, és közölte, hogy Brovko találkozót kér tőle: „A Patriarsije Prudinál. Nem kell bemenni sehová, csak egy séta lesz." Néhány óra múlva Vjarja azt válaszolta, ezt a kérdést a cég vezetőivel kell megoldania. Ekkor már maga Brovko írt neki:

*Szia. Mintha abban állapodtunk volna meg, hogy néha kapcsolatba lépünk egymással – a feletteseid bevonása nélkül. Tudnánk ma találkozni?*

Vjarja: *Szia. A főnök azt kéri, hogy rajta keresztül döntsek, ahogy ő fogalmaz*

Brovko: *Nocsak. Miért?*

Vjarja: *Rendkívül elégedetlen, hogy a feje fölött ugrálunk, általában Vartan (Hacsaturov) szokta felhívni és ő tárgyal vele*

*Én csak egy beosztott vagyok és a főnököm hozzájárulása nélkül nem tudok*

Brovko: *Akkor mondd azt, hogy kávét inni mész ki*

Vjarja: *Sajnálom, nem tudok* ☺

Brovko: *Ez nem igaz, na jól van*

*Add meg a főnököd számát*

Ljaminnak nem tetszett az egész. Csetelni kezdett a Telegramon „WTF" néven, a csoportba meghívta Vjarját, Brovkót és Hacsaturovot.

Ljamin: *Kollégák. Jó napot. Mondtam hogy dühös vagyok – de mintha semmit se mondtam volna.*

Hacsaturov: *Szia*

Ljamin: *Vartan, én mindig örülök, ha segíthetek neked. Te ezt tudod. De, amikor a fejem felett piszkálják kollégáim – ELLENZEM*

Hacsaturov: *Becsületemre mondom hogy azt gondoltam, ez egy egyszeri eset* ☺

Ljamin: *Beleegyeztem a Szófiának való segítségnyújtásba. Se többe, se kevesebbe. Az összes fennmaradó „kreativitást" nem hagytam jóvá. Várom Vaszilij Brovko hozzászólását és magyarázatait.*

Hacsaturov: *Kollégák, csak nyugodtan* ☺

Ljamin: *nyugodtan dühöngök. úriemberek így nem viselkednek*

Brovko: *Nem értem, hogy összességében miről is van szó. Nekem Gyenyisz [Vjarja nem tudja, hogy ő kicsoda – a szerző megjegyzése] azt mondta, hogy az én konzulenseim vagytok egy nagyon kényes kérdésben. De ha nem, hát nem*

Hacsaturov: *Vaszilij, Gyenyisz azt nem mondta, hogy ez elhúzódhat, és nem egyszeri segítség* ☺

Brovko: *Egyszeri segítség. 15 perc a hotelben*

Hacsaturov: *Nekem úgy tűnt, hogy akkor ez nem probléma, Szás*

Ljamin: *Én nem tudtam, hogy mi ez a tizenöt perc és hogy miért ez a tizenöt perc*

Hacsaturov: *Egyszerűen egyet kell értsek veled*

Ljamin: *Akármi is történjék, ő az én munkatársam, akinek én fizetem a munkaidejét. Akkor miről is van szó? Nekem van kontaktom – akkor velem is dolgozz. Nem a 15 percről van szó. Hanem arról, hogy az általam fizetett emberek engem megkerülve találkoznak. Ez megengedhetetlen.*



Hacsaturov: *Jól van, Szás, nyugodj meg, kérlek. Ez félreértés, és mi őt már beszabályoztuk* ☺

Ljamin: *Remélem, hogy meghallottatok és megértettetek.*

Vjarja elmondása szerint ezután Brovko és a munkatársai nem fordultak többé hozzá.

* * *

Írtam Vaszilij Brovkónak arra a Telegram-elérhetőségre, amelyen keresztül felajánlotta Vjarjának, hogy találkozzanak a kibertámadás megtárgyalása kapcsán. Szinte azonnal válaszolt, hogy Vjarja *„Bulgáriában a kiberfenyegetések elleni védelmi rendszer analízise miatt volt, nem pedig ilyen támadások véghezvitele kapcsán". „Nem fogom kommentálni azokat a vádakat, amelyek túl vannak a józan ész határain, és amelyeknek közük sincs a valósághoz* – tette hozzá Brovko. – A *Rosztech folyamatosan ki van téve a kibertámadásoknak – az év elejétől a konszern vállalatainál több mint tizenegyezret hajtottak végre."*

Vjarja főnöke, Alekszandr Ljamin tárgyalni hívott a Qrator Labs irodájába. Kiderült, hogy a tornacipős, tarka pólós, szakállas ember víg kedélyű és beszédes – ő megerősítette, hogy a Minkomszvjaztól, az orosz kommunikációs és távközlési minisztériumtól Hacsaturov bízta meg Vjarját, hogy találkozzon Vaszilij Brovkóval. „A beszélgetés egyáltalán nem a DDoS-támadáshoz szükséges rendszerről folyt, hanem a hálózati forgalomgenerátorról – arról a rendszerről, ami elengedhetetlen ahhoz, hogy ellenőrizni lehessen a weboldalak stabilitását leterheltség esetén –, mondta Ljamin, több mint valószínű, hogy a Szlonra zúdítottak össztüzet. Kísérleti jelleggel, ellenőrzésképp. Hogy ez nem legális? Ez szürke zóna."

Ljamin azt feltételezte, Vjarja valamiért megsértődött a cégére, és lehetséges, hogy amikor a *Rosztech* megrendeléséről beszélt, azt végül az ő legfőbb konkurensük, a Kaspersky Lab teljesítette. „Finnországban a dollárral lehet kezdeni valamit" – mondta Ljamin, és átküldött egy

hivatkozást[3] a Reuters értesüléseiről, amelyek szerint Jevgenyij Kaszperszkij arra szólított fel, hogy „mártsák be a konkurenciát". Ljamin hozzátette, nem biztos benne, hogy Vjarja „egészséges".

2015 tavaszán a Qrator teljes gárdája Csehországba készült. Vjarja és a családja átköltözött a csernatovi bérelt lakásából Birjulevóba, hogy kicsit takarékoskodjon a külföldi út előtt.

Május végén Vjarja ismerős autót vett észre az irodánál: a festett furgont az antennákkal, amelyik először akkor jelent meg a cég épületénél, amikor a Qrator Navalnij weboldalán dolgozott. Néhány nappal később meglátta ugyanazt az autót a háza mellett. Vjarja „kezdett paranoiás lenni": az volt az érzése, mintha ugyanazokkal az emberekkel találkozott volna a város különböző részein. Elhatározta, otthonról a munkahelyére különböző mikrobuszokkal fog utazni.

Július utolsó napjaiban Vjarja jelezte a cége vezetőségének, hogy nem fog tudni elutazni Csehországba, mert ellenzi a felesége. De Ljamin szerette volna, ha munkatársainak lennének európai irataik, ezért azt tanácsolta Vjarjának, szerezzen be személyi igazolványt Finnországban, ahol apai ágon rokonai voltak. A személyi igazolványért vizsgát kellett tenni finn nyelvből. Vjarja szabadságot vett ki, hogy megtanulja a nyelvet.

Ezzel párhuzamosan, ahogy Vjarja mesélte, ismerőseitől hallotta, hogy továbbra is érdeklődnek iránta a Rosztech és a titkosszolgálat munkatársai, hogy valahogy mégis bevonják abba a kiberfegyverkezési munkába, amit egyszer már látott működés közben. Vjarja maga is biztos volt abban, hogy ez így fog történni – különben „fejbe fogják kólintani".

2015 augusztusában a titkosszolgálatokkal kapcsolatban álló barátai azt tanácsolták neki, hagyja el Oroszországot. A következő napon összeszedte két útitáskába a holmiját, és elutazott Helsinkibe.

* * *



2015. augusztus 25-én kora reggel Vjarjával megérkeztünk a helsinki rendőrségre, ahol politikai menedékjogot kérelmezett. A hivatal még zárva volt, az épület mellett néhány iraki menekült várakozott. Egy rövid interjú és ujjlenyomatvétel után Vjarját elküldték az egyik menekülttáborba: egy Helsinki központjától nem messze eső, háromemeletes épületbe, ahol ingyenes menza is működött. A házban és a ház körül tucatnyi iraki és szíriai járkált, és közben kivétel nélkül mindegyik telefonált.

Beköltözése után Vjarja egy csecsenföldi menekülttel beszélgetett. Ő azt ajánlotta neki, vigyázzon a kimosott holmijára, mert a táborban lopnak. Másnap összeismerkedett egy szibériai párral, akik bűnvádi eljárás elől rejtőzködtek, illetve egy bizonyos egyiptomi miniszter intelligens fiával. A harmadik nap ezt a férfit elszállították a táborból malária gyanújával. A negyedik nap azt mondták Vjarjának, hogy a bevándorlási hivatal munkatársaival folytatott hosszabb interjú után több mint valószínű, hogy átviszik egy Helsinkitől hatszáz kilométerre északra fekvő menekülttáborba – ügyében épp a döntésre várnak.

Így is történt. Ezt követően Vjarját másfél éven keresztül egyik táborból a másikba hurcolták, és időről időre kihallgatták. Nem nagyon korlátozták a mozgásában, segélyt fizettek neki, amiből nehezen ugyan, de meg lehetett élni.

Története érdekelni kezdte a finnországi ukrán követséget – az ukránokkal való találkozásakor Vjarja elmesélte, hogyan zajlott a védelmi minisztériumuk weboldala elleni támadás. A Rosztech és az orosz nyomozószervek Vjarja nyilatkozataira hivatalosan semmit nem reagáltak.

* * *

2016. december végén a *The New York Times* címlapon közölt egy rövid cikket Vjarjáról azokra az anyagokra hivatkozva, amelyeket én készítettem a *Meduza* számára (később az újság Pulitzer-díjat kapott az Oroszországról szóló anyagainak sorozata miatt, ezt a cikket is beleértve). A szövegben

Vjarját „elit hekkernek" nevezték. Vjarja csodálkozott, és ezt írta nekem: „elit hekker, azt a kurva, honnan veszik?" A cikk megjelenése után behívták a soron következő beszélgetésre a finn titkosszolgák, és megkérdezték, hogy mit tud az orosz hekkerekről és a finnországi energetikai rendszer nemrégiben történt feltöréséről.

2017 nyarán Vjarja végre megkapta a finn politikai menedékjogot. Szeptember elején, két évvel azután, hogy elmenekült Oroszországból, találkoztunk. Nem ismertem meg. Húsz kilót fogyott, és olyan ember benyomását keltette, mint aki ledobta magáról az őt hosszú ideje gyötrő terhét.

Vjarja elmesélte, a finn menekültügyi rendszerben eltöltött másfél év nem volt könnyű. Egyszer végezni is próbált magával, de a barátai időben közbeavatkoztak, és kórházba került néhány hétre. A pénze kevés volt, nem volt módja a családegyesítésre, a kihallgatások rengeteg időt elvettek. Az egyetlen öröme a horgászás volt, aminek a kedvéért gyakran egy egész napot biciklizett. Vjarja szomszédai a migrációs központokban főleg irakiak és szíriaiak voltak, akik az Iszlám Állam elől menekültek. A legtöbbjük antidepresszánsokat szedett, sokuk sebesült volt. Többen azt gondolták Vjarjáról, hogy a központ munkatársa.

Sört és rövidet ittunk, aztán Vjarjával elsétáltunk az egyik városszéli folyóhoz: valahol azt olvasta, hogy ott jó a kapás. „Most már mintha itthon lennék. Mindent elrendeztem, a klíma is nekem való – mondta a programozó. – Mintha már nem is emigrációban lennék, ez az én új életem." Kinyitott egy fémdobozkát, egy kicsit kutakodott a felszerelései között, azzal bedobta a horgászbotját a vízbe.

***

A Vjarjával való találkozás után néhány héttel az egyik moszkvai kávézóban ismerős hangra lettem figyelmes. Megfordultam, és megláttam Vjarja egykori főnökét, Alekszandr Ljamint. Interjút adott valakinek, és először nem ismert meg, amikor pedig üdvözöltem, elkapta a tekintetét. Amikor kifelé ment, ismét köszöntem neki. Szabadkozott, hogy amikor először üdvözöltem őt, azt gondolta, túlságosan hangosan beszél, és ezzel esetleg zavar engem a munkámban.

Ljamin örült, amikor hallotta, hogy Vjarjának sikerült megoldania a papírjait. A cég munkatársainak nagy része addigra már Prágába költözött: onnan kényelmesebb kiszolgálni az ügyfeleket a kibertámadások kivédésére épülő szolgáltatásokkal. A beszélgetés végén Ljamin megkérdezte: „Mit gondolsz a Mihajlovval, az FSZB-vel és a hazaárulással kapcsolatos történetről?" (Nem sokkal azelőtt az FSZB egy magas rangú munkatársa kiberbűncselekményt hajtott végre, és hazaárulás vádjával letartóztatták.) Mint kiderült, Ljamin sokat törte a fejét ezen az utóbbi időben.

Vjarja története azon ritka esetek közé tartozik, amikor egy ember nyíltan beszél arról, milyen érdekeltségei vannak az orosz államnak és a titkosszolgálatnak a kiberfegyverkezésben. Nem elképzelhetetlen, hogy Vjarja az egyetlen, aki megtagadta az ilyesfajta fegyverkezéssel kapcsolatos megbízást, és el tudott tűnni komolyabb következmények nélkül (már ha nem tekintjük annak a korábbi életének a teljes feladását, beleértve a családjától való elszakadását is).

2017 őszére Vjarja finnre cserélte a kereszt- és családnevét, elköltözött, telefonszámot, postacímet és Telegram-fiókot váltott. Most arról álmodik, hogy vesz egy nagy csónakot, amellyel a legmélyebben úszó lazacokra halászhat. A munkát illetően nem távolodott el eredeti foglalkozásától: létrehozott egy civil szervezetet, amely azt figyeli, hogy egyes államok hogyan hajtanak végre kibertámadásokat más államok ellen.

*I. rész*

# Gyökerek

*1. fejezet*

# A szabadság területiuma

1992-ben egy szentpétervári fiatal, egy bizonyos Kirill először látogatott ki[4] a város délnyugati peremén lévő Junona piacra. A bolhapiac még az ezt megelőző évtizedben létesült: a Junij Technik* áruház körül gyűltek össze az emberek, hogy a járdákra kipakolt rádióalkatrészeiket árulják. A piacgazdaság beköszöntével az elkerített terület mellett is létesültek elárusítópultok, de a piac megőrizte specialitását: alapvetően elektronikai eszközökkel és azok kiegészítőivel kereskedtek itt. Az egyik legnépszerűbb látványosság egy tizenöt perces bemutató volt az Atari nevű számítógépes játékhoz használt konzolon.

Mint sok más szentpétervári, Kirill is ezen a piacon vette az első saját számítógépét, és rengeteg időt töltött a gép előtt. Néhány évvel később a fiatalember rövid időre az Egyesült Államokba utazott, ahol akkor lett épp egyre népszerűbb az internet. Kirill Kaliforniában használt először böngészőt. A hazájába visszatérve észrevette, hogy a kint megismert számítástechnikai underground Oroszországban is fokozatosan kiépül, és elhatározta, megosztja az emberekkel az Amerikában szerzett tudását arról, mi is az a www, az FTP és az IRC.**

Kirill nemsokára összeismerkedett a számítógépek és az internet többi, szintén az elsők közé tartozó orosz szerelmeseivel. Magukat „szcénának" nevezték, körülbelül har-

* Az áruház neve, a Junij Technik szóösszetétel fiatal technikát jelent. – *A fordító megjegyzése.*

** Lásd *Fogalomtár.*

mincan voltak, és a legtöbbjük Moszkvában vagy Szentpéterváron élt. 1995-ben először gyűltek össze az Enlighton, a számítógép-kedvelők konferenciáján. Többek között a merevlemezek távolra dobásában rendeztek versenyt. Egyébként egymással alapvetően az IRC-chaten keresztül találkoztak – és ez az érintkezés sokukat megváltoztatta.

„Oroszország utcái akkoriban jóval kevésbé voltak barátságosak, mint manapság. A beszélgetések legnépszerűbb témája mindig maga az élet volt. Ebbe minden belefért, a nőktől a kozmoszig – mesélte a szcéna egyik képviselője. – Konkrét témák nem voltak, és mindez azért volt fantasztikus, mert mi lettünk a világon az elsők, akik az érintkezéshez elsősorban az internetet használtuk. Amikor [1997-ben] Diana hercegnő életét vesztette – ez éjszaka történt –, a csatornán mindenfelől voltak fent emberek. Közülük az egyik abban a [párizsi] kerületben élt, ahol az események történtek. Odament, körülnézett, és visszatérve mesélni kezdte az élményeit. És mindössze nyolc óra elteltével az egész világ erről tárgyalt, miután megnézte a híradásokat."

Ezekben az években az egyik legnagyobb problémát a számítógéphez való hozzáférés jelentette: ez néha még azoknak sem volt egyszerű, akiknek volt otthon gépük. A programozó Anton Melnyikov részletesen visszaemlékezett[5] arra, milyen mesterkedésekhez kellett folyamodniuk a barátjával, Misával, hogy számítógépes játékokkal játszhassanak – például lógtak az iskolából. Eleinte beteget jelentettek, amihez tintasugaras nyomtatón nyomtattak igazolást. „Betegnek nem tudtam mindig tettetni magam, mivel nálunk lakott a nagymama, ezért reggelente nagy kínok közepette muszáj volt felkelni és elindulni, mintha iskolába mennék. Olykor azt hazudtam, hogy csak a második-harmadik órára kell mennem, de ezt túl gyakran nem lehetett megcsinálni, hisz voltak besúgók – mesélte Melnyikov. – Az iskola helyett Misához mentem, de ott is volt probléma: az ő házuk gyakorlatilag szemben volt a sulival. Mivel ugyanabban az időben minden osztálytárs és tanár



szintén az iskolába ment, kénytelenek voltunk kémeset játszani: óvatosan haladtunk, köröztünk, elbújtunk a hóbuckák mögé stb."

Voltak más nehézségek is. „Misánál az apja felfedezte [a játékoktól és az internettől való] a függőséget, és összeszerelt egy csodaeszközt, ami a számítógépnek csak egy kulcs használatával adott áramot – emlékszik vissza Melnyikov. – Misa a kulcsot természetesen ellopta, és másolatot készített róla." Amikor a barátjának az apja egy nap hazaért, és felfedezte, hogy a monitor forró, onnantól elkezdte dugdosni a tápegységet, ám a kamaszok pótlásképpen vettek egy másikat. Aztán Misa apja a kamrába tette a monitort. „De erre is találtunk megoldást. Az ajtón nagy rések voltak, mi pedig egyszerűen megtanultuk levenni az ajtót a sarokvasáról – folytatja Melnyikov. – A legszörnyűbb az volt, ha valaki csengetett. Ekkor gyorsan ki kellett kapcsolni a monitort, betolni a kamrába, az ajtót pedig a helyére rakni."

Ennek eredményeképp a barátok csaknem egy teljes negyedévet lógtak a tanévből. „A lelepleződésünk életem egyik legszégyenteljesebb momentumával ért véget – mondja Melnyikov. – Megaláztak minket az egész osztály előtt. És ezt minden tanárunk sorban újra megtette. Különösen az igazoláshamisítás nyugtalanította őket. Azt jósolták, hogy pénzhamisítók leszünk." Melnyikov ezután otthon, éjszakánként játszott, miután bonyolult szisztémát dolgozott ki, amelyik kikapcsolta a számítógép hűtési rendszerét, hogy ne zúgjon, és ezzel ne keltsen gyanút a szüleiben. Ennek csak egyetlen szépséghibája volt: a gép túlhevült, és Melnyikov egyszer arra ébredt, hogy a szobában égésszag terjeng.

Nem kellett hozzá sok idő, hogy a kamaszok megszerezzék a hozzáférést a hálózathoz. „A romló tanulmányi eredményem tudatában senki nem szeretett volna fizetni az internért, ám megvolt a megoldás – a Metakom nevű szolgáltatónál megjelent a »vendég-hozzáférés«. Ez egy

ingyenes hozzáférési lehetőség, ahol helyi szerveren lehet IRC-zni és közben FTP-zni. Az időt nem korlátozták, de nagyon bonyolult volt telefonon keresztül elérni. Köszönetet szeretnék itt mondani azoknak az embereknek, akik ezt létrehozták. Nagymértékben járultak hozzá, hogy sorsom új irányt vegyen, és hosszú évekre szólóan segítettek rátalálni önmagamra. Tulajdonképpen folyamatosan a gépnél dekkoltam. Barátokra tettem szert, és fokról fokra számítógép-specialistává váltam."

Hasonlóan alakult más orosz fiatalok élete is, akik előtt megnyílt a számítógépek világa. Egyesek gyorsan felfogták, hogy ezzel még keresni is lehet: annál is inkább, mivel – ahogy erre Kirill visszaemlékszik – az első hekkerek közül nagyon sokan rajongtak az akkor divatba jövő rave-ekért, illetve a narkotikumokért, amelyek beszerzéséhez pénzre volt szükségük. A hekker szavai szerint a „szcénához tartozók" először warezzel foglalkoztak,* vagyis számítógépes kalózkodással. Mások a napjaikat arra pazarolták (az azokban az időkben lassú internettel), hogy népszerű programokat töltöttek le, azokat kiírták CD-re, és eladták őket.

A következő időszakot a hitelkártyaadatok ellopása és a zárt hálózatok feltörése jelentette – ez jóval több pénzt hozott, mint a kalózkodás. A STEALTH csoport résztvevői azt mesélték,[6] hogy már 1994-ben behatoltak az amerikai követség rendszerébe, magukat „harcias robotgyilkosok létrehozóinak nevezve a kiberfelületeken". Kollégáik visszaemlékeztek,[7] hogyan törték fel Novorosszijszk weboldalát és hogyan szereztek hozzáférést az ukrán parlament számítógépeihez. Maga Kirill egy ponton megalapította a Sodom nevű hekkercsoportot, amelynek a jelmondata így hangzott: *„Russian maffia – we'll take care of you."***

* Lásd *Fogalomtár.*

** Az angol mondat értelme magyarul: „Orosz maffia – mi majd a gondodat viseljük!" – *A fordító megjegyzése.*



„A kilencvenes években Oroszország és Ukrajna olyan volt, mint egy megvadult méhkas. Mindent lehetett csinálni, ami csak kedvünkre való volt, mivel nem volt semmiféle törvényi szabályozás – emlékszik vissza az 1990-es évek eleji hekker-underground egyik résztvevője. – Mindenki irigyelte a szabadságunkat. Oroszországban nem volt korlátozás, mint Európa vagy az Egyesült Államok gyerekeinél. Világszerte tiszteltek bennünket és féltek tőlünk, mert Oroszország fiatalembereinek feltörekvő nemzedéke ösztönös félelmet keltett bennük a fegyverekről, a vodkáról, a sötét utcákról és egyéb dolgokról szóló sztorijaival."

*2. fejezet*

## Hogyan károsították meg Ászja nénit?

*Ez a mi világunk, a kódok és elektromos impulzusok világa, amely tele van a kommunikációs eszközök hangjainak szépségével. Mi ingyen használjuk azokat a szolgáltatásokat, amelyek amúgy is csak pár kopejkába kerülnének, ha önök nem üzérkednének a szükségleteinkkel és nem volnának annyira mohók – és maguk még minket neveznek bűnözőknek. Mi bőrszínre, nemzetiségre és vallásra vonatkozó előítéletek nélkül élünk – önök mégis bűnözőknek hívnak minket. Önök állítják elő az atombombát, szítanak háborút és ölnek; meglopnak és megkárosítanak mindenkit, miközben igyekeznek meggyőzni minket a saját igazukról – de mi mindannyian bűnözők maradunk. Igen, bűnös vagyok. A bűnöm a kíváncsiság. A bűnöm az, hogy én az embereket a tudásuk, a gondolataik és a tetteik alapján ítélem meg, és nem az alapján, hogy hogy néznek ki. A bűnöm az, hogy okosabb vagyok önöknél, amit nem tudnak nekem megbocsátani. Én hekker vagyok, és ez az én kiáltványom. Önök le tudnak állítani közülünk egyeseket, de mindannyiunkat nem tudnak leállítani.*

2003-ban a *Hekker* orosz kiadása közölte[8] a kódtörők e manifesztumát, amely először tizenhét évvel korábban jelent meg egy amerikai netes kiadványban, a *Phrack*ben. Az orosz verziót olvasók számára a benne foglaltak eddigre már rég közismert tények voltak. Ekkorra a „számítógépes huligánok" kiadványa már öt éve virágzott, és elérhető módon magyarázott el mindent, amire csak vágytunk: hogyan lehet feltörni az elektronikus levelezést, hogyan lehet DDoS-támadást szervezni, és hogyan lehet ellopni hitelkártyaadatokat.



A *Hekker* első példánya 1998-ban jelent meg a Gameland kiadó jóvoltából (a cég alapvetően folyóiratokat és videójátékokat adott ki), és igen hamar sok orosz diák és egyetemi hallgató kultikus tárgya lett. A havilap hasonlított William Powellnek *The Anarchist Cookbook* (Anarchista szakácskönyv) című munkájára. Az 1970-es évek elején a fiatal és elvetemült Powell, aki úgy vélte, az ismereteket mindenki számára elérhetővé kell tenni, és azok alapján az emberek majd képesek maguk meghozni észszerű döntéseiket, megírta és kiadta kézikönyvét, amelyben elmagyarázta, hogyan kell robbanóanyagot készíteni bárki által elérhető összetevőkből, valamint hogyan kell megfigyelés alá vonni és megölni embereket. A következő évtizedek során a könyvre gyakran bukkantak rá terroristák és gyilkosok lakásaiban, például azoknál a kamaszoknál is, akik az amerikai Columbine gimnáziumban lövöldöztek (maga Powell végül tanár lett, és hosszú éveken keresztül próbálta megtiltani, hogy újra kiadják a munkáját).

A *Hekker* első számában hitelkártyák feltörésére vonatkozó instrukciókat közöltek, a másodikban tanácsokat adtak ahhoz, hogyan kell ellopni a fiókot az ICQ üzenetküldő alkalmazásról (az írás címe *Hogyan károsítsuk meg, illetve védjük meg Ászja nénit* volt), és szerepelt még benne egy cikk a feltörésekhez szükséges programok jegyzékéről. „A hekkerkedésnek két módja létezik – írta a szerző. – Az első: veszel egy halom könyvet az internet felépítéséről és működéséről, a programozási nyelvekről, az operációs rendszerekről, a protokollokról, a processzor működéséről stb. Ha mindezt figyelmesen elolvasod, két év gyakorlás után minden rést látni fogsz, és képes leszel megszerezni minden számodra szükséges infót különösebb probléma nélkül. De hiszen te lusta vagy! [...] Épp ezért válaszd a második módot: hadd olvassák a könyveket és írjanak programokat más srácok, én pedig learatom a munkájuk gyümölcsét. Na és aztán, így van jól, ez nem is kérdés!"

Volt cikk a „legtermékenyebb hekkerekről," és azokról

az internetes helyekről, ahol nulladik napi támadásokat lehetett vásárolni.* A lap olyasvalaki visszaemlékezését is közölte, aki feltörte egy bank biztonsági rendszerét, és tanácsokat adott, hogyan ne kerüljünk a titkosszolgálat karmai közé. De közöltek hírességekkel készített interjúkat is – például a Delfin nevű énekessel, aki a hekkerséget „extrém sportnak" nevezte, és elismerte, hogy ő maga is szeretett volna „feltörni valamit."

A *Hekker* hatodik számában a kritikus infrastruktúra sérülékenységéről (megtámadhatóságáról) beszéltek, sőt véletlenül megjósolták olvasóik jövőjét is. „Az információs háborúk a 20. század végén olyannyira reálissá váltak, hogy egy meghatározott pillanatban ki lehet majd robbantani a harmadik világháborút úgy, hogy ki se megyünk otthonról, csak ülünk a számítógépünk klaviatúrája előtt – írta a cikk szerzője. – És hogyha eddig a védelmi minisztériumok különös figyelmet fordítottak a szárazföldi, légi és tengeri határaikra, akkor mostanra kialakult még egy határ: a virtuális. És vajon ki fogja védeni ezeket a határokat? Véleményem szerint a felnövekvő hekkerek, akik megunták, hogy ingyen foglalkozzanak minden szarsággal; a tudásukat a titkosszolgálatnál vagy a védelmi minisztériumnál akarják használni, virtuális határőrökként, szemmel tartva minden olyan elektront, amely kontinensről kontinensre vándorol."

A magazin alternatívát kínált a szerényebb lehetőségű kisvárosi orosz kamaszoknak, akiknek nem volt különösebb elfoglaltságuk. „Úgy érzed, nem jutott neked az égvilágon semmi. Ez baj, de könnyen lehet orvosolni – válj hekkerré!" – mondta ki nyíltan az egyik lapszám. A tipikus jövendőbeli hekker, aki a 2000-es évek elején úgynevezett kártyásként, vagyis bankkártyás csalásokkal és hamisításokkal kezdte (azaz pénzt csalt ki a bankkártya-tulajdonosoktól), az 1990-es években egy szibériai városban nőtt fel: a szovjet időkben az ilyen város egy nagyipari vállalat köré épült, de a Szovjetunió széthullása után a gyár bezárt, és a lakosság nagy többsége munkanélküli lett. Ez a kamasz a város egyetlen újságosához járt, és mindig megvette a *Hekker* legfrissebb számát. Az eladónő már arcról felismerte, és nyújtotta is felé a lapot. „Lehet, hogy csak ez az egyetlen példány jutott el hozzánk – emlékezett vissza egy kódtörő a velem folytatott beszélgetésekor. – Talán ostobán hangzik, de a *Hekker* olyan volt, mint amikor valaki friss levegőhöz jut a fojtogató szmogban."

A *Hekker*t Moszkvában is olvasták. Ilja Hofman az 1970-es évek végén született értelmiségi családban: az apja zeneszerző volt, anyja is művészettel foglalkozott. Gyerekkorában Iljának heveny allergiája és asztmája volt, ezért otthon tanult. A kisfiú zenei tehetsége hamar megmutatkozott – hegedűn és brácsán játszott –, de a matematikai is: lelkesedett az algebráért, kamaszkorában publikált is néhány diákköri dolgozatot matematikai tematikájú folyóiratokban. Az iskola után Hofman a Csajkovszkij Moszkvai Konzervatóriumba felvételizett, ahol egyik tanára Jurij Basmet volt. Az 1990-es évek végére Hofman számított[9] az egyik legreményteljesebb és legtehetségesebb akadémiai növendéknek.

1998 tavaszán kezdett lelkesedni a *Hekker* iránt. Hofmannak leginkább a *Feltörés* rovat tetszett meg, amelyben azt tárgyalták, hogyan kell ellopni a hitelkártyák adatait, és kijátszani a bankok védelmi rendszerét. Ahogyan később mondta: „Minden elérhető [volt], mint a mesében." A hekkerség a fiatalember számára „az emberi képzelet csodálatos jelenségének" tűnt, romantikus foglalkozásnak. „Az egy dolog, hogy az ember játszik a számítógépes

* A szövegben a továbbiakban gyakran szereplő „a nulladik napi támadhatóság vagy sebezhetőség" azt jelenti, hogy kiküszöbölhetetlen támadás érkezik egy kártékony programon keresztül az adott számítógépes rendszerre, olyan, amely ellen még nem fejlesztettek ki védelmi mechanizmust. Vagyis amely ellen nulla nap áll a fejlesztők rendelkezésére, hogy elhárítsák a hibát. – *A fordító megjegyzése.*

játékkal és nem képes kiszállni belőle – magyarázta Hofman később. – Ez érthető is: a kifejlesztett játék egyszerűen csodás. A hekker azonban benne él a virtuális világban, és nem a számítógépes valóságot figyeli, hanem annak belső világát. Ennek az embernek, aki a fekete képernyőt és a kacsintgató kurzort látja, elég, hogy azt érezze, ebben a pillanatban valóban ott tartózkodik. Olyan volt, akár egy rejtvény, és szórakoztató volt vele foglalkozni. Ez számított a soron következő matematikai feladatnak, igen, annak a határán voltunk, hogy pénzt keressünk vele, de végül nem éltünk ezzel. Számomra úgy tűnt, hogy ez a morált sem sérti. Hiszen a banki rendszerben mindennek megvan a kompenzációs mechanizmusa, azaz minden helyreállítható."

Hofman felvette a NetSerpent (internetkígyó) álnevet, és rátalált a csapatára. Együttműködve sikerült átutalniuk a saját számláikra körülbelül 97 ezer dollárt tizenhat amerikai és néhány orosz bankból. A kártyák adatait egy kanadai internetes webáruház feltörése után kapták meg. A gyanús aktivitást annak az orosz banknak a biztonsági munkatársai észlelték, ahol a csapat tagjai a számláikat vezették. A bűnözőket nem kellett sokáig keresni: mindegyik számlát ők nyitották meg a saját, valódi nevük alatt.

A lopott pénzen a hekkerek mobiltelefont vásároltak (akkor ez luxusnak számított), illetve Versace- és Calvin Klein-holmikat. Hofmannak még költenie sem sikerült: 1998 őszén mindnyájukat őrizetbe vették, és a fiatal hegedűművészt mint a csoport feltételezett szervezőjét börtönbe vitték. A *Moszkovszkij Komszomolec* című lapban „internetes kígyóknak" nevezték őket.[10]

Hofman védelmére Jurij Basmet kelt, aki őt „nemcsak az osztálya egyik legjobb hallgatójának" nevezte, hanem „Moszkva egyik legjobb fiatal brácsásának". „Meg kell tenni mindent, ami lehetséges, hogy megőrizzük a tehetségét hazánk kultúrája számára" – emelte ki a zenész. Ennek (és asztmája) ellenére, Hofman fél évet ült a Matrózcsendnek nevezett, hetven férőhelyes cellában – ahol folytatta a zeneszerzést.

A bíróság a fiatal moszkvait és tettestársait feltételesen öt évre ítélte. Szabadsága visszanyerése után Hofman a IV. Nemzetközi Jurij Basmet-brácsaverseny díjnyertese lett, és folytatta zenei karrierjét, megnyerve még néhány, brácsásoknak szervezett világversenyt. Jelenleg a moszkvai Gnyeszinka zenei szakközépiskolában tanít, és gyakran lép fel koncerteken.

*3. fejezet*

## A kétségek félelemmé váltak

Az első orosz hekkerek nem csupán a fórumokat és a szaksajtót befolyásolták, hanem a popkultúrát is. Hisz róluk, akik a számítógépek előtt ülve sorsokat és államokat irányítottak, fantasyket írtak és Hollywoodban filmeket forgattak. A filmek közül az első még 1983-ban készült, *Háborús játékok* címmel. Az egyik hekker, aki a világ minden táján titkos dokumentumok után kutatva tört fel vállalatokat, azt mesélte, hogy gyerekkorában ez a mozi óriási hatással volt rá. A történet szerint egy kamasz hekker, miután behatolt az amerikai katonai hivatal hálózatába, ott olyan fájlokat talált, amelyekről azt hitte, videójátékok: *Légi harcok, Hadműveletek városi körülmények között, Háború a pusztaságban, Globális termonukleáris háború.* Végül a dolog majdnem a harmadik világháborúba torkollott. Amint a *Háborús játékok* kijött, komolyan megrémisztette[11] az USA akkori elnökét, Ronald Reagant, aki ezután adta ki a megbízást, hogy dolgozzák ki az automatikus információs rendszerek nemzetbiztonsági stratégiáját – az erről szóló titkos utasítást 1984-ben írták alá.

Az 1990-es évek közepén Hollywood figyelme ismét a hekkerek felé fordult. Az *Adatrablók* indította be Angelina Jolie karrierjét, és arról szólt, hogyan harcolnak egy alvilági kibercsoport tagjai a multinacionális cégek kapzsi munkatársai ellen. Amikor 2004-ben nagyszabású közvélemény-kutatást[12] tartottak az orosz nyelvű hekkerfórumok látogatói körében, kiderült, hogy épp ez a film hatott rájuk a legerősebben, és ez késztette őket arra, hogy elgondolkodjanak az identitásukon és a gazdasági globalizációval szembeni ellenálláson.



*Az Adatrablók* videókazettán szinte azzal egy időben jutott el Oroszországba, hogy a fantasyíró Szergej Lukjanyenko megírta regényét A visszatükröződések labirintusa *(Labirint otrazsenyij)* címmel a virtuális világokban dolgozó „búvárokról". Kiberpunk jellege ellenére a könyvben sok minden realisztikus volt: az internetes portyázások közötti szünetekben a hős kolbászos szendvicset evett. Sőt, a regényben még a hekkerek romantikus himnusza is benne volt:

*A munkánk a sötétségben folyik*
*Tesszük, amit tudunk*
*Visszaadjuk, amink van*
*A munkánk a sötétségben folyik.*
*A kétségek félelemmé váltak*
*A félelem pedig a sorsunkká.*
*Minden egyéb – művészet*
*Az őrületben az légy, aki vagy.*

Az interjúalanyaim közül páran azt mesélték, jól emlékeznek arra a különbségre, ami az 1990-es évek hétköznapi orosz valósága – amikor még kolbász se jutott mindenkinek – és az internet határtalan lehetőségei között volt érzékelhető. A kilencvenes évek végére a hekkerfórumokon már kialakultak a saját profillal, sőt saját szubkultúrával rendelkező közösségek: voltak, akik verseket írtak, voltak, akik elbeszéléseket. Írtak „titkos instrukciókat is a hekkerek számára" arról, hogyan kell kifogástalanul kinézni abban az esetben, ha az újságírók mégis lefotóznának. Egy ilyen instrukció a következőképp festett:

1. Leülni minden olyan készülék elé, ahol van monitor és billentyűzet.
2. Vegyél fel szemüveget!
3. Tekinteteddel megkérni a kezelőt, hogy fordítsa úgy a kamerát, hogy a képernyő visszatükröződjön a szemüvegen.
4. Bökj rá bármelyik billentyűre, hogy megjelenjen a Pentagon feltörésének teljes képernyős kódja, a feltörés lépéseivel.

5. Szívasd meg a legnagyobb pofájú IT-sokat!
6. Tördeld vagy ropogtasd az ujjaidat.
7. Mind a tíz ujjaddal fénysebességgel kezdd el nyomkodni a klaviatúrát *enter* és szóköz nélkül, tíz másodpercig.
8. Pár másodpercre állj meg, és mondd azt, hogy bemértek minket.
9. Dupla fénysebességgel nyomkodd újra a billentyűzetet, hogy kikerüld a tűzfalat.
10. Hajolj előre és töltsd le: Így, ni, ez az, bakker, én vagyok az Isten.
11. Utalj át magadnak 99999999999999999999 USD-t.
12. Az 5 évnyi IT-s tanulmányok megtérülnek.

A hekkerfórumokon ennél jóval kifinomultabb művészi projektek is létrejöttek. 1999 végén ilyen fórumokon kezdett terjedni a *Történet, amely nem létezett, avagy a '99-es haknuty* választások* című színdarab.[13] A darab hősei a korszak legaktívabb hekkerei közül kerültek ki, és arról meséltek, hogyan törték fel az orosz választási rendszert.

MeteO> *munka van, sok dolcsiért*

Leshy> *és hány évet adhatnak ezért?*

MeteO> *neked biztos a legtöbbet*

Leshu> *na, mesélj*

MeteO> *biztosan képben vagy, hamarosan választások lesznek?*

Leshu> *a-ha ... a „Jabloko" – Rulez!*

MeteO> *semmi nem oké, egyáltalán, tudod, hogy hogy épül fel a GASZ-vibori? ***

Leshu> *elvileg igen. Ocsmány az egész. Kitaláltad, hogy feltöröd?*

MeteO> *hogy te mennyire éleselméjű vagy ma!*

Leshu> *világos. Kinek a rendelése?*

* Az orosz *haknuty* kifejezést olyan hekkertechnológiákra alkalmazzák, amikor a feltörők megszerzik a hozzáférést a más által birtokolt információkhoz. – *A fordító megjegyzése.*

** A GASZ-vibori a választások informatikai rendszere Oroszországban.



MeteO> *Berezovszkijé.*

Leshu> *hogy átnyomjuk Putyint, Sojgut, Gurovot és Karelint?*

MeteO> *ne vitatkozz. Guszinszkij embereivel párhuzamosan kontaktolunk – nekik szintén nincs ellenükre, hogy bőkezűen adakozzanak*

Leshu> *egyáltalán nem szeretném a legjobb esetben is mankóval végigsántikálni a maradék életemet*

Meteo> *hogy mennyire bírsz pánikolni...*

A darab vége felé volt egy jelenet az egyik elemzőműsorról, amelyet a valóságban akkoriban az ORT-n (most ez az 1-es tévécsatorna) Szergej Dorenko vezetett. „Amint az ismert a központi választási bizottsághoz és az FSZB-hez közeli hírforrásokból, valószínű, hogy a *GASZ-viborib*a behatolt egy hekkercsoport – közölte a műsorvezető a darabban. – Amint azt láthatják az osztankinói Föderális Információs Centrum *99-es Választások* eredményjelző tábláján, amelyről a választók által preferált pártok grafikonja legálisan letölthető, öt százalékkal nőtt az *Egység* és a *Jabloko* népszerűségi indexe is."

Ezt követően a történet szerint kitör a káosz: *„A nép őrjöngeni kezdett. Minden egyes tévécsatornán azt közvetítették, hogy a már bezárt választóhelyiségekben is dulakodás zajlott, provokálva ezzel bizonyos politikai erők oldalán álló ideges embereket, és a nép szó szerint széttépte a szavazólapokat a felnyitott urnáknál. Általános pánik és fejetlenség vette kezdetét."*

Akkoriban a hekkerfórumok látogatói ilyen történeteket csak kitalálni voltak képesek. Húsz évvel később – az USA 2016-os elnökválasztásán – az álmaik majd valóra válnak.

*4. fejezet*

## Diákok feltörik a NASA-t

A hekkerek nagy többsége kezdetben csak szórakozásból foglalkozott feltörésekkel: ellopták a szüleik számítógépének a jelszavát, feltörték a szomszéd internetes hozzáférését, elorozták a barátaik ICQ-ját. Ahogyan azt az egyik interjúalanyom megállapította: „kiderült, hogy az ICQ ellopásától a kiberháborúban való részvételig nincs is olyan sok lépés".

„[Az 1990-es évek közepén] az internet globális jelleget öltött, és Oroszországban is lefedett már minden régiót. A hekkerek úgynevezett kétes üzelmeiről először csak külföldről lehetett hallani, vagy a moziban lehetett ilyeneket látni, de a mieink se sokat késlekedtek – emlékezett vissza[14] az egyik hekker, aki ezekben az években kezdte meg a működését. Oroszországban nemsokára megszervezték a számítógépes bűnözés elleni küzdelem ügyosztályát, a moszkvai újságokban megjelentek azokról a »kis hekkerzsenikről« szóló cikkek, akik akkor épp a börtönbüntetésüket töltötték. Valójában szegény gyerekeket fogtak el; egyetemistákat, akik csupán keresni szerettek volna egy kis pénzt az interneten, és hamis hitelkártyákkal akartak rendelni maguknak árucikkeket (a valódi hekkerséghez az ilyesmi soha nem tartozott). Amíg az FSZB emberei ezek után a »hekkerek« után futkostak, mások nyugodtan ültek otthon, és teljes biztonságban juthattak újabb ismeretekhez. Oroszországban a hekkerség hatalmas sebességgel bontakozott ki, ráadásul semmilyen akadály sem hárult ez elé a hatóságok részéről."

1998-ban pár barát az Előzetes letartóztatás cellája néven



alapította meg saját csoportját – de gyakrabban nevezték magukat (az orosz kifejezés rövidítéseként) KRZ-nek. „Éppen amikor kamaszok ezrei nézték meg az Oroszországba is eljutó *Az adatrablók* című filmet, és olvasni kezdtek cikkeket a témáról, rárohantunk az internetre, és azt képzeltük magunkról, hogy professzionális feltörők vagyunk" – emlékezett vissza[15] a csoport egyik tagja. A KRZ öt-tíz tagból állt. Első dolguk az volt, hogy bosszút álljanak az Orkok nevű ismert moszkvai számítógépes körön, amelynek adminja egyik barátjuknak „némi erkölcsi kárt" okozott. A csoport a cég szerverét törte fel. A továbbiakban a KRZ megrendelésre teljesített még néhány feltörést, de amikor az orosz interneten már „semmi vonzó nem maradt", elkezdtek az amerikai kormány internetes erőforrásai iránt érdeklődni. Ahogyan azt a *Hekker* egyik számában a csoport tagjai megerősítették,[16] huszonegy amerikai weboldalt törtek fel,[17] közöttük egyetemek, katonai intézmények, valamint a NASA honlapját is.

A KRZ hekkerei szívesen meséltek magukról: egyikőjük bevallotta, hogy tizenöt éves, és a tizedik osztályban tanul. „Mondhatjuk, hogy jó tanuló vagyok. ☺ Hármas-négyes vagyok – írta[18] abban cikkben, ami a *Hekker*ben 1999-ben megjelent. – Egyébként az iskolánkban nincs informatika tantárgy. Micsoda iskola is ez. ☹ Mindent magamnak kell kikutatnom: sok könyvet olvasok a különböző számítógépes témákban, rengeteg dolgot kikísérletezek mindenféle segítség nélkül. Arra készülök, hogy internetszolgáltatónál fogok majd dolgozni."

Egyszer a KRZ egyik tagjánál elment az áram. Kopogtak az ajtón.

– Ki az? – kérdezte a hekker.

– Rendőrség! Nyissa ki.

– Mivel kapcsolatban?

– A számítógéppel.

Amikor bementek a lakásba, a rendőrök lefoglalták a számítógépét, és a csoporttagot bevitték az őrsre. Ott ki-

nyitották a számítógépen az ICQ-t, tanulmányozták, de „csak rejtélyes szavakat láttak". Miután feltettek a fiatalembernek néhány protokolláris kérdést – „még azt sem tudták, hogy mit kérdezzenek" –, a rendőrök hazaengedték.

A hekkertársadalom fejlődésével párhuzamosan folyamatosan kezdett formálódni a piac is, ahol meg lehetett vásárolni a szolgáltatásaikat. Dmitrij (kérésére megváltoztattam a nevét) a 2000-es évek elején kezdett érdeklődni a feltörések iránt, amikor tizenhárom éves volt: a számítógépének nem volt elég kapacitása a játékokhoz, de valamivel foglalkozni akart. Először az osztálytársával készítettek weboldalakat: a barátja lerajzolta az iskolai füzetébe az órákon a dizájnt, aztán Dmitrij közvetlenül a papírra írta a kódot. „Az ilyen korlátok kedveztek a találékonyságnak, bennem pedig elég gyorsan kialakult az érdeklődés az iránt, hogy hogyan lehet az ilyen weboldalakat feltörni" – emlékszik vissza a hekker.

Az első áldozatai más tanulók weboldalai lettek. Nem sokkal ezután rátalált a hekkerfórumokra. Akkoriban sok ilyen volt: a hackzone.ru, amelyből aztán a betiltott Underground Information Center nőtt ki (a Hackzone őslakosainak nem tetszett, hogy a weboldalnak kamaszok lettek a rabjai, ezért úgy döntöttek, külön felületet alakítanak ki maguknak), a bugtraq.ru, a void.ru. Dmitrij az Antichat[19] törzsvendége lett, ahol a hálózatokat, a feltöréseket és az információs védelem híreit tárgyalták meg. Ugyanúgy, mint más fórumok tagjainál, az Antichat látogatóinak egy része szinte a weboldalon élt, sőt még dalt is szentelt neki:[20]

*Korán kelve bekapcsolom az internetet*
*Belépek az Antichatre, a világon jobb*
*weboldal nem is lehet*
*Antichat.ru, Antichat.ru*
*Érted minden weboldalt bedöntök*
*Antichat.ru, Antichat.ru*
*Azért mert szeretlek téged*



A fórumon a hozzáférésnek volt szintjei: a soron következőre mindig úgy lehetett felkerülni, ha valaki egy cikkben bebizonyította, hogy jártas a programozásban. Ahogy az Antichat hierarchiájának csúcsára jutott, Dmitrij összeismerkedett más fiatal hekkerekkel. Néhány évvel később közülük kerültek ki Oroszország legjobb kibervédelem-specialistái, mások jól keresnek az illegális feltörésekkel, és vannak, akik a börtönbüntetésüket töltik az USA-ban. Maga Dmitrij végül elhatárolódott a feltörésekkel való pénzkeresettől, mert nem volt képes „magából paranoiást nevelni": „Hiszen ez folyamatos stressz, mindig óvatosnak kell lenni."

Fórumbéli kollégáinak ilyen problémái nem akadtak, és nyíltan ajánlották szolgáltatásaikat minden érdeklődőnek. Sok hasonló weboldal manapság is létezik, ezeken változatlanul lehet találni kereskedelmi ajánlatokat: pénzért lehet venni vírust, meg lehet rendelni közösségi oldalak vagy szinte bármilyen messenger (kivéve a Telegram) feltörését, valamint közeli hozzátartozóink megfigyelését, továbbá DDoS-támadás megszervezését vagy a GTA5-játékban elért pontszám hamis megnövelését. A hirdetés így néz ki:[21]

*Megtudjuk az eredeti felhasználói nevet és a jelszót, így AZ ÁLDOZAT NEM FOG TUDNI A FELTÖRÉSRŐL. Távolról feltörünk bármely számítógépet, és megszerezzük a hozzáférést bármilyen adathoz vagy információhoz a számítógépen. A nap huszonnégy órájában dolgozunk.*

*Szolgáltatásokat nyújtunk weboldalak és szerverek eltávolítására DDoS-támadás segítségével. Profi privát programokkal dolgozunk, amelyek megsemmisítik, akadályozzák, felborítják, vagy egy időre leállítják az ön által megrendelt erőforrásnál a weboldal vagy a szerver munkáját. Segítségünkkel ki tudja iktatni a konkurenciát vagy az ellenséget, amely keresztezi az útját vagy zavarja önt a bizniszben. Az ár és a minőség viszonya nálunk a legjobb a DDoS-szolgáltatások piacán, forduljon hozzánk.*

A hekkerek általában a kliensek számára anonimitást, hosszú távú együttműködés esetén árengedményt és „személyre szabott" szolgáltatást ígértek. Az egyik hekker azt mondta nekem, hogy a jövedelme legfőbb részét a jelszavak megrendelésre történő feltörése teszi ki. Ahogy ő fogalmazott, az ilyen munka sok pénzt hoz, és általában nagyon egyszerű elvégezni, hiszen a legtöbb ember változatlanul az *1234567*-hez vagy a *qwerty*hez hasonló jelszót használ.

*5. fejezet*

## Iskola a feltörők számára

Mialatt az első hekkerek a saját közösségeiket szervezték, újfajta tevékenységeikre az állam is kezdett felfigyelni. Az 1990-es évek végén és a 2000-es évek elején a legtöbb műszaki egyetemen megjelentek az információvédelmi tanszékek. Ezek közül a legerősebbek az MGU-n,* az MFTI-n,** a Bauman Egyetemen, a pétervári LETI-n*** és azokon az egyetemeken, ahol információs technológiát, mechanikát és fénytant tanítanak. E felsőoktatási intézmények végzett növendékei iránt a 2000-es évek közepére az új munkaerőpiacon nagy volt a kereslet: a cégek tömegével kezdték alkalmazni az úgynevezett „pentestereket" (azokat, akik a vállalat informatikai védelmét tesztelik kibertámadási modellekkel).

A kibervédelem matematikusai, programozói és szakemberei már a 2010-es évek közepére hatalmukba kerítették a világot. Befolyásuk évről évre nőtt, mivel folyamatosan emelkedett az állampolgárok megfigyelésére, a személyes információk megsértésére és egyéb adatok begyűjtésére szolgáló eszközök száma. Ezeket a matematikusokat a kutatók például a WMD *(weapons of math destruction)***** alkotóinak nevezték.[22]

* Az MGU a Moszkvai Állami Egyetem rövidítése.
** Az MFTI a Moszkvai Műszaki Fizikai Egyetem rövidítése.
*** A LETI a szentpétervári Állami Elektrotechnikai Egyetem rövidítése.
**** Szójáték: a „weapons of mass destruction", azaz a tömegpusztító fegyverek szóösszetétel mintájára a „weapons of math destruction" kifejezés a matematikai modellekre épülő kibertámadások pusztító erejére utal. – *A fordító megjegyzése.*

Egyébként az orosz számítógépes képzés egyáltalán nem a nulláról indult. Még az 1960-as években az elit szovjet matematikai iskolák és azok a főiskolák, ahová a matematikai iskolák végzett növendékei jelentkeztek, készítették fel a nemzetközi olimpiák győzteseit és a jövő sikeres tudósait. Ez a rendszer folyamatosan egészült ki a fiatal matematikusok és informatikusok számára külső helyszínen szervezett táborok és gyűlések szerteágazó hálózatával. Ezek az intézmények fennmaradtak a Szovjetunió szétesése után is. Éppen ezeknek köszönhető, hogy az orosz kamaszok éveken át megnyerték a programozó világbajnokságokat. Az egyik interjúalanyom szerint az orosz hekkerek éppen az erős képzésnek köszönhetően váltak a legjobbakká a világon: még ha maguk a konkrét feltörők nem is tanultak matematikai líceumokban vagy főiskolákon, így vagy úgy mégis ezt az iskolát képviselték.

„Ebben az egész történetben kiemelten fontos a matematika szerepe – fejtegeti Andrej Lopatyin, a pétervári ITMO* egyetem munkatársa és a fiatal orosz programozók trénere. – Minden siker közvetlenül az erős orosz matematikai iskolához köthető. A pétervári matematikai iskola ebben hatalmas szerepet játszik, különösen a 239-es líceum és az Anyicskov-palotához köthető körök. Én ott kezdetben az informatikai feladatokat papíron oldottam meg. Ide járt Nyikolaj Durov is." (Nyikolaj a VKontakte és a Telegram alapítójának, Pavel Durovnak a testvére, ő felelt mindkét projekt programozásáért.)

A Nyári Számítógépes Iskolába – amelyet júliusban és augusztusban a Kosztroma városához tartozó egyik szanatóriumban tartanak – évente kétszáz diák érkezik a világ minden országából (a nyári iskolának van egy téli változata is). Az odautazást gyakran a regionális hatóságok vagy a nagy orosz internetes társaságok fizetik, a Yandex

* Az ITMO a szentpétervári Nemzeti Kutatóegyetem rövidítése.



vagy a VKontakte: ezekhez sokan mennek a Nyári Számítógépes Iskola végzett növendékei közül dolgozni diploma után. Az iskolában algoritmusokkal, az adatok struktúrájával és elméleti informatikával foglalkoznak. A kamaszok mindennap négy órában tanulják a matematikát, ebéd után pedig önállóan oldanak meg feladatokat.

„A szovjet és az orosz matematikai iskolák mindenekelőtt nagyon erős oktatáson kívüli foglalkozások – magyarázza Lopatyin. – A matematikai iskolákban a hagyományos iskolai tantervek határait meghaladó dolgokról van szó. Az itt folyó munka a gondolati összefüggések gyors kombinációját segíti mind a szellemi erőfeszítéseket igénylő versenyeken, mind az egyesületi munkában, de minden más területen is."

Azaz, például, feltörések esetén is. Egy orosz hekker, aki annak idején részt vett a Nyári Számítógépes Iskola kurzusain, úgy emlékszik, ott tanult meg gyorsan gondolkodni és eredeti megoldásokat kieszelni. Hatodik osztályos kora óta érdekelte a tiszta matematika, de ahogy folyamatos hozzáférése lett a számítógéphez, az informatika iránt kezdett lelkesedni. Amíg informatikaórán az osztálytársai a *Need for Speed*en játszottak, ő a programozási nyelveket tanulmányozta, és az első saját programjait írta. „Játszani mindig tudtam – a matematikaórákról azért engedtek át a számítástechnika-csoportba, mert nem volt mit csinálnom – emlékszik vissza egyik interjúalanyom. – Az én foglalkozásaim ott voltak: például a fejben számolás. A tanárnő tudta, hogy nem játszani járok, hanem valami értelmeset csinálok." A Nyári Számítógépes Iskola után beiratkozott a Bauman nevét viselő MGTU* információs védelmi karára, de még be sem fejezte, amikor hamarosan jó pénzre tett szert az egyszerű feltörésekkel, amelyekre a fórumokon keresztül kapott megrendeléseket.

* Az MGTU Moszkvai Állami Műszaki Egyetem rövidítése.

A Nyári Számítógépes Iskola nem az egyetlen iskolán kívüli képzés a tehetséges kamaszkorú programozók számára. 2017 nyarán Petrozavodszkban találtam magam – ez Karélia fővárosa, az Onyega-tó partján fekszik, és telente itt tartják a legtekintélyesebb IT-képzéseket: egy héten keresztül körülbelül félszáz tanuló versenyez egymással; feladatokat oldanak meg, és készülnek a nemzetközi programozóolimpiára. „A petrozavodszki találkozók a legrégebbiek – meséli az egyik szervező, Andrej Sztankevics. – Hogy miért éppen a mi gyerekeink ennyire éles eszűek? Többek között azért, mert a Szovjetunióban kiépítették a matematikai iskolák hálózatát, majd a programozás oktatását és rendezvényeit is ezek mintájára hozták létre."

Sztankevics, aki fiatalon megnyert néhány informatikai olimpiát, a 2000-es évek közepén kezdte vezetni a programozók gyűléseit, és ekkor állt az élére a pétervári ITMO csapatának is, amelyik másokhoz képest jóval többször nyerte meg az orosz versenyeket. Az ő szavai szerint az olimpiákon és versenyeken elért győzelmek után az állam is elkezdett érdeklődni a fiatal programozók iránt. Sztankevics még egy Vlagyimir Putyinnal való találkozón is részt vett: ahogyan azt az orosz elnök kifejtette, az ilyen rendezvények remekül illeszkednek ahhoz, hogy a sportprogramok finanszírozásának bővítéséhez megtaláljuk a lehetőségeket. E nyilatkozat után vették be a programozást azon diszciplínák sorába,[23] amelyeket Szocsiban, a tehetséges gyerekek számára létrehozott Szíriusz táborban fognak a későbbiekben tanítani. A tábort Putyin kezdeményezésére alapították.

2013-ban – folytatja Sztankevics – a kamaszkorú informatikusok iránt „intenzíven érdeklődni kezdtek" a védelmi minisztérium katonái. Kezdetben nem volt könnyű dolguk [a védelmi minisztérium katonáinak]. „A minisztériumban sok a korlátozás a mozgás és minden egyéb területén. Nálunk viszont a gyerekek kozmopoliták, és mobilisak akarnak lenni – magyarázza Sztankevics. – Mégis, tudom, hogy pár gyerek, aki ott volt a nyári iskolákban, most az FSZB akadémiáján tanul."

Idővel a védelmi minisztérium és a vele kapcsolatban álló szervezetek (például az információbiztonsági szolgálatok vezetőinek szövetsége [ARSIB], amelyet a KGB és az FSZB korábbi munkatársa, Viktor Minyin vezet) elkezdték megrendezni a saját hekkerversenyeiket. Ezeken meghatározott idő alatt kellett feltörni egy bizonyos rendszert. A versenyek résztvevői a szünetekben meghallgatják a védelmi és a hírközlési minisztérium munkatársainak előadásait, akik „az információs tér leendő védelmezőinek előkészítéséről", a CIA struktúrájáról és a hekkercsoportokról beszélnek.[24]

Borisz Mirosnyikov, aki sok éven át vezette a Belügyminisztériumban a kiberbűnüldözés nyomozati osztályát, még 2005-ben az egyik kiberbűncselekményekről szóló konferencián kijelentette,[25] hogy „az orosz hekkerek a legjobbak a világon". „Ezek a tegnap még kamaszok, akik mindenféle szisztéma nélkül foglalkoztak a hekkerséggel, mostanra felnőttek, és tökéletesítették a módszereiket. Korábban ezzel pimasz kölykök foglalkoztak. Most már felnőttek – mondta a rendőrtisztviselő. – Felfogták, hogy ha valamiben jól kiismered magad, akkor használnod kell ezt, azért, hogy megkeresd a kenyeredet. Hekkerekké váltak, és a hálózaton keresztül egyesültek, hogy meggazdagodjanak. Közismert tény, hogy az oroszok erősek a matematikában. A programozóink a legjobbak a világon, ezért a hekkereink is a legjobbak a világon."

*6. fejezet*

## A végzett növendék

A műszaki egyetemeken végzett hallgatók többsége a szó szoros értelmében nem válik hekkerré. Ők a végzettségüknek megfelelő tudományos kutatóintézethez (orosz rövidítésük: NII) szerződnek, amely a védelmi minisztériummal áll kapcsolatban (ezekről az intézményekről a 27. fejezet fog részletesebben szólni), vagy magánkézben lévő IT-cégeknél helyezkednek el, amelyek a 2000-es évek elején futottak fel Oroszországban. Egyébként néhányan közülük legálisan ajánlják fel megközelítőleg ugyanazokat a szolgáltatásokat, amelyeket a kiberbűnözők árulnak a saját fórumaikon: például emberek megfigyelését.

A 2000-es évek első évtizedének közepén Moszkva egyik legerősebb matematikai iskolájában – a délnyugati 1543-as számúban – tanult egy magas és mosolygós nebuló, Artyom Kuharenko. Az iskoláig helyközi autóbusszal a Moszkva melletti Troickból jutott el: az út általában másfél órát vett igénybe oda-vissza – a Vnukovo repülőtér, az új moszkvai adminisztrációs körzet, illetve az MKAD (a moszkvai körgyűrű) érintésével.

Kuharenko ötödik osztályos kora óta járt informatikaszakkörre, nyaranta számítógépes iskolákba járt, ahol az algoritmikus programozást, az adatok struktúráját és analízisük módszereit tanították. 2006-ban megnyerte az összoroszországi levelező informatikai olimpiát. Az iskola után Kuharenko az MGU-ra felvételizett matematika és kibernetika szakra, még csak nem is gondolt más lehetőségre. Másodéven a *Bevezetés a számítógépes látásmódba* speciális



kurzusra járt, és ugyanennek az évnek a végén egy megbeszélés után bekerült a számítógépes grafika és multimédia tanszék laboratóriumába. A negyedik évfolyamhoz közeledve a laboratórium vezetőjének tanácsára Kuharenko egy új és addig nem kutatott terület felé fordította a figyelmét: az arcfelismerés felé.

Az egyetem elvégzése után Kuharenkónak különböző munkahelyei voltak, és gyakran utazott. 2015-ben a téli szünet alatt nagyon sok szabadideje lett, és unalmában egy alkalmazást készített, amely a kutyafajtákat fotó alapján képes meghatározni. Barátnőjével együtt szétterítettek fotókat mintegy százötven kutyafajtáról, és megtanították a Kuharenko által fejlesztett neurális hálózatot a kutyafajták felismerésére. Az alkalmazás nem vált népszerűvé, de a következő tavasszal Kuharenko lehetséges befektetőkhöz fordult. Azt mondta nekik, hogy az arcfelismerésre képes neurális hálózatok jelentik a jövőt, és 2020-ra ez a piac hatmilliárd dollárra fog nőni. Páran hittek neki, így jött létre a NtechLab nevű cég.

A projekt egyik befektetője és kurátora Alekszandr Kabakov volt, Vaszilij Brovko barátja, a Rosztech munkatársa, azé az állami konszerné, amelyik Alekszandr Vjarja állítása szerint DDoS-támadást hajtott végre a slon.ru weboldal ellen. Kabakov és Brovko sokszor utazott és pihent együtt: a Facebook-bejegyzéseik alapján 2016-ban majdnem minden hónapban. Rajtuk kívül volt még egy befektető, Makszim Perlin, aki kapcsolatban állt a Kreml-barát ifjúsági mozgalmakkal: az ő legismertebb projektje nem volt más, mint az MGU egyetemista lányairól készült erotikus naptár, amelyik 2010-ben jelent meg, Vlagyimir Putyin születésnapjára.

2015 tavaszán Kuharenko cége beköltözött a moszkvai Tyisinszkaja tértől nem messze található, jelentéktelen bevásárlóközpont kis irodáiba. Az NTechLab egy teljes emeletet foglalt le, de az irodák üresek voltak, bútor is alig

akadt bennük. A cég első beruházása során darabonként néhány millió rubelért négy szervert szerzett be, ebből hármat a programozók asztala alatt helyeztek el, egyet pedig egy különálló hűtőhelyiségbe tettek. Kuharenko, aki külsőre Edward Snowdenre hasonlít, mosolyogva dicsekedett: „A Google ezekre a célokra ezer szervert használ, nálunk mindössze négy van."

Ők írták meg azt az algoritmust, amelyet FaceN-nek neveztek el: ez az a neurális hálózat, amely saját maga tanulja meg és talál rá az emberek felismeréséhez szükséges megkülönböztető jegyekre az arcon: a szemek nagyságára, a szemöldök ívelésére, az ajkak formájára és egyebekre. A hálózatot egymillió fénykép alapján tanították meg: algoritmusa már 2015 tavaszán jobb eredményeket mutatott, mint a Google-é: a pontosan felismert arcok 73,3 százalékával szemben az ottani 70,5 százalék állt. Az egyik programozóversenyen elért győzelem után a céget elhalmozták az algoritmus vásárlására vonatkozó ajánlatokkal: többek között meg akarta venni Törökország határőrszolgálata, hogy megállapíthassa, kik kelnek át a szíriai határon. Az orosz titkosszolgálatok részéről is érkeztek ajánlatok: a moszkvai hatóságok úgy döntöttek, hogy hozzákapcsolják az algoritmust a több mint tízmillió videókamerából álló városi rendszerhez. „Azoknak az embereknek az [arcát], akik elhaladnak a kamerák előtt [az algoritmus segítségével], ellenőrzik a rendszerbe feltöltött, a bűnözőket vagy az eltűnt embereket tartalmazó adatbázison keresztül – magyarázta Kuharenko. – Hogyha nagyfokú hasonlóság mutatkozik, akkor előzetes figyelmeztetést küldünk a rendőrség munkatársának. Ugyanezt az algoritmust kezdték használni Moszkvában az ellenzéki akciók résztvevőinek felismerésére is.

Ezzel párhuzamosan Perlin azt ajánlotta Kuharenkónak, hogy próbálja meg kivinni az algoritmusát a tömegpiacra is. Együtt kigondolták a Findface-t, azt az alkalmazást,



amelynek segítségével lehetővé válik, hogy fénykép alapján bárki accountját megtaláljuk a VKontaktén. „Ez teljesen törli az anonimitást – írta[26] Perlin, miközben bemutatta az alkalmazást a saját Facebookján. Ha ön észrevesz egy szimpatikus lányt a buliban, és lefotózza a telefonjával, pillanatok alatt megtalálja a profilját a VKontaktén, s miután onnan megismerte a nevét és az érdeklődési körét, már küldheti is neki az üzenetet." Az alkalmazást majdhogynem azonnal elkezdték másra is használni: az anonim 2ch fórumon például megjelent az az üzletág, amely olyan „bőrök" keresésére szólított fel, akik pornót forgattak és prostituáltként dolgoztak. Az alkalmazást a rendőrség is használni kezdte: előszedtek régi ügyeket, feltöltötték a Findface-re a gyanúsítottak fényképeit, amelyeket a VKontaktén találtak, aztán a felhasználók minden adatát lekérték a hálózatról.

Kuharenkót mindez nem zavarta, úgy vélte, a biztonság fontosabb a privát életnél. Kérdeztem őt a Jarovaja-csomagról: éppen 2016 nyarán fogadott el az orosz parlament, az állami duma egy törvénytervezet-csomagot, amely jelentősen megkönnyítette a biztonsági tisztviselőknek az interneten található személyes adatok elérését. „Köpök az egészre – reagált a programozó. – A közösségi oldalakon én mindent kitárgyalok. Hadd olvassa csak az FSZB, kivel feküdtem le, és milyen csajok voltak nálam. Hivatalos levelezés? Hát tudják csak meg, mennyit keresek és milyenek az ügyfeleim. Őszintén szólva szerintem ez senkit sem érdekel. A privát szféra problémája fel van nagyítva. Bármely telefonszámhoz való hozzáférés magától értetődő, hát hadd olvassanak engem a titkosszolgálatok."

2018-ban az NtechLab által kidolgozott arcfelismerő rendszer működésbe lépett Moszkvában. Ahogyan azt a város polgármestere, Szergej Szobjanyin nyilatkozta, a rendszer révén a metróban már nyárra több mint tíz, körözés alatt álló személyt tartóztattak le. Egyiküket, aki az ellen-

zéki Másik Oroszország Párt aktivistája, azt mesélte, hogy az őt letartóztató rendőröknél volt egy speciális eszköz, amelyen rajta volt az ő térfigyelő kamerával készített fényképe, de még a neve, a születési dátuma és a nyilvántartási címe is. Az adatlapja pirosan világított és „cincogott": kiderült, hogy a körözöttek nyilvántartásába őt a szélsőségesek elleni küzdelemre szakosodott központ munkatársa vette fel. A férfi megkérdezte a rendőrt, hogyan tudná töröltetni magát ebből a nyilvántartásból. A rendőr azt felelte: „Sehogy."

*II. rész*

# Pénz

*7. fejezet*

# A hekkerek bolygója

Amíg az Egyesült Államokban a dotcomok aranyláza folyt, az orosz hekkerek – többségükben még kamaszok – a saját valóságukat hozták működésbe: az amerikai kereskedelmi hálózatok hitelkártyáinak, a bankok és az internetes webáruházak adatainak ellopása sokuknak dollármilliókat hozott. Amikor az Egyesült Államokban egy kiváló programozói készséggel megáldott ember adatlopás nélkül is tízezer dollárt kereshetett, a volt Szovjetunióban, ahol rengeteg ember csupán néhány száz dollárt keresett évente, a csábítás túlságosan nagy volt.

Az orosz hekkerek közül az első, aki nemzetközi hírnévre tett szert, a pétervári Vlagyimir Levin volt, aki az 1990-es évek közepén egy amerikai banktól több tucat millió dollárt emelt el. Elég gyorsan lefülelték, a futárokat pedig, akik az összeget készpénzre váltották, letartóztatták. Levint kiadatták az Egyesült Államoknak, ahol harminchat hónapot töltött a börtönben, ami nevetséges idő, ha összevetjük azzal, amennyit mostanában a hekkerek kapnak. Nem sokkal később Levin történetének bizonyos motívumai alapján forgattak néhány epizódot egy banditákról szóló orosz filmsorozathoz, ám maga a hekker, miután visszatért Moszkvába, eltűnt – már húsz éve senki nem tudja, hol van, és mivel foglalkozik.

A feltörés iparága a 2000-es évek elején kezdett megváltozni az erre szakosodott fórumok megjelenésével, amelyek a csoportok átszerveződése miatt folyamatosan megújultak. „Korábban a hekkercsoportok inkább érdeklődésen alapuló közösségekbe tömörültek. Az emberek nagyjából

ugyanazzal foglalkoztak, egyszerűen tapasztalatokat cseréltek, és valamely kérdés megoldásához egyesítették az erőiket – mesélte[27] ezekről az évekről Andrej Szporov, aki SpORaw néven maga is hekker volt. – Most a csoportok gyakran egy konkrét üggyel kapcsolatos munkára szerveződnek. Pár feladat teljesítése után a csoport megalakultnak tekinthető, elég sokáig fennmaradhat, és büntetlenül foglalkozhat a tevékenységével, mert a külső kapcsolatai korlátozottak: minden szakember a csoporton belül van. Fennmaradtak olyan csoportok is, amelyek a régi elvek mentén épültek fel, de ott olyan újoncokat »nevelnek«, akik miután tapasztalatra tettek szert az érdeklődési körüknek megfelelő munkában, azon kezdenek gondolkodni, hogy anyagi érdekből új kompetenciákat sajátítsanak el."

Szporov arról beszélt, hogy a 2000-es évek elején az orosz internet némileg hasonlított az 1990-es évek orosz utcáira. „Ebben az időszakban a tőke elsődleges felhalmozása zajlott azoknál, akiknek soha nem voltak ilyen lehetőségeik, amíg legálisan dolgoztak – magyarázta. – Az intellektuális bűncselekmény sokkal kevésbé érhető tetten, mint a hétköznapi jellegű. A későbbiekben a felhalmozott pénzt be lehetett fektetni teljesen szokványos kereskedelmi projektekbe is, ezek közül néhány még ma is létezik."

A 2000-es évek elején a kiberbűnözők fő közössége a világon az orosz CarderPlanet nevű fórum volt, amelyet Bolygónak is neveztek: ahogyan azt az egyik hekker fejtegette nekem, sokuk számára a weboldal valóban helyettesítette a reális világot.

Minden a carder.ru-val kezdődött, amelyet a 2000-es év elején egy magát *Script*nek nevező személy hozott létre. A *Hekker*ben közölt néhány publikációja miatt a látogatóinak a száma hamarosan elérte a napi hatszázat is – akkoriban ez soknak számított. Script nemsokára bezárta a fórumát és megalapította a CarderPlanetet, de a két felület célja azonos volt: itt kereskedtek az ellopott hitelkártyákkal, vagyis a „kartonokkal", ahogyan ezeket a fórumon nevezték. A weboldalra körülbelül ezer ember regisztrált. 2001-ben Script kisajátította a fórumon a „Törvényes tolvaj"* státuszt: a bálványa Szasa Belov volt, az akkor még csak nemrégiben bemutatott *Brigáda* (Brigád) című sorozatban szereplő kitalált bűnözőtekintély, akit Szergej Bezrukov játszott.

A Bolygó nemsokára az összes orosz nyelvű cyber-underground érintkezés legfontosabb helyévé vált: a bankkártyás csalókon (kártyásokon) kívül a spammerek, a trójaiak fejlesztői, az exploiterek, a PayPal-fiókok feltörői egyaránt itt érintkeztek, meg azok is, akik irathamisításra specializálódtak. A hekkerek információkat és módszertant cseréltek a feltörésekről, és arról tárgyaltak, hogyan védjék meg magukat a megfigyeléstől. A fórumon feltűnő újoncok közül sokan úgy gondolták, lehetőségük adódott a gyors pénzszerzésre.

A maffia mintájára a fórum tagjai „családnak" nevezték magukat, és belső hierarchiát építettek ki a klán elvei alapján. Scriptet nemcsak „Törvényes tolvajnak", hanem „Keresztapának" is nevezték. A fórum egyik vezetője így ábrázolta[28] ezt a hierarchiát:

*Sgarrista:* regisztrált felhasználó.

*Don:* családtag.

*Capo Bastone:* a család barátja és a Keresztapa „jobb keze".

*Gabellotto:* a főbíró, a biztonsági szolgálat feje.

*Consigliere:* a család tanácsadója a legkülönfélébb fontos kérdésekben.

*Capo di Capi:* olyan tagok, akire a család védelmének és segítésének missziója hárul.

*Capo:* azok a megbízható emberek, akikre figyel a kor-

* Ez a státus az 1930-as évektől kezdve kizárólag a szovjet (majd az orosz) bűnözői alvilágban létezik, a világ más országaiban ismeretlen. Olyan bűnelkövetőkre vonatkozik, akik az alvilág elitjéhez tartoznak, és ebben a körben tekintélyt vívnak ki maguknak. – *A fordító megjegyzése.*

mányzat, illetve olyan emberek, akik nem vesznek részt a fórum életében.

*Giovane d' Honore:* a fórum moderátora.

*Ripper:* kidobóember.

*Scum of Society:* a közösség söpredéke, a státuszt a leggyakrabban az érdemelte ki, aki a moderátorokat vagy a tagokat alázta.

*Harkály:* az az ember, aki jogot formál magának arra, hogy egyidejűleg legyen jelen a különböző felületeken, hogy ostoba kérdéseket tegyen fel, megzavarva ezzel a többi tag érintkezését.

„A hekkerek feltörték az amerikai online áruházak és az elektronikus tranzakciós rendszerek védelmét, és adatokat gyűjtöttek a kliensek hitelkártyájáiról – mesélte[29] a CarderPlanet egyik tagja. – Mindez jól jött a kártyásoknak, akik a saját csatornáikon keresztül készpénzt tudtak csinálni a kártyaadatok használatával. Azután, hogy az információk beszivárogtak a nyomtatott sajtóba, és az újságírók elkezdtek írni egy újfajta jelenségről, lehetőség nyílt a gyors meggazdagodásra egyetemi hallgatók tömegének bevonzásával. Az amerikai plázák többségének még nem volt tapasztalata kártyásokkal, ezért nem okozott gondot az esetszám növelése az újoncoknak sem. A nép gyakran rendelt, sokat, és egyfolytában."

A Bolygó állandó lakóinak nagy többsége körülbelül ötezer dollárt keresett havonta,[30] a weboldal alapítóinak és más veteránjainak a jövedelme viszont elérhette akár a százezret is. Ezt a pénzt ingatlanokba fektették, ezekből nyíltak meg aztán a gumiabroncsműhelyek és a virágüzletek.

Script elmagyarázta,[31] hogy a kártyás tevékenység egyben szórakozás is: „Annál az embernél, aki kockáztat, termelődni kezd az úgynevezett boldogsághormon. Ez a hormon, amely megsokszorozódik a papírpénzek susogásának hatására, alapvető és döntő szerepet játszik abban, hogy az ember ezt a nem teljesen tisztességes szakmát űzze. Ezzel foglalkozni nem szégyen. Legyen csak szégyen a kormányunknak, hogy a kamaszok már ilyen fiatalon tolvajjá válnak." Script ekkor már együttműködhetett az ukrán titkosszolgálatokkal is. A fórum tagjai úgy emlékeztek, Script említést tett arról, hogy az SZBU (Ukrán Biztonsági Szolgálat, az FSZB ukrán megfelelője) szereti őt.



2002-ben a CarderPlanet Odesszában konferenciát tartott a hitelkártyás csalóknak. A konferenciára körülbelül húsz ember érkezett. Sétálgattak a városban, elmentek szaunázni, éttermekben vacsoráztak és a szervezeti kérdésekről tárgyaltak. A konferencia résztvevői közül sokan elragadtatva tértek haza, hiszen most először ismerkedhettek meg azokkal, akikkel éveken át csak online érintkeztek.

Ugyanekkor jelent meg a fórumon egy Boa (oroszul Udav) nevű felhasználó. Hamar sztárrá vált: a hekkerségről és a hitelkártyacsalásról szóló cikkei mintha az életről meséltek volna. A legnépszerűbbé az etikettről szóló cikke vált: ezt Boa azután írta meg, hogy a fórumra százával kezdtek kamaszok regisztrálni, miután olvastak a Bolygóról a *Hekker*ben (a CarderPlanet veteránjai közül voltak, akik arra kérték Scriptet, hogy ne reklámozza a felületet, de ő erre azt válaszolta, hogy a „pénz az interneten mindenre elég", és a „hatóságoknak mi nem kellünk"). Az újoncok jelentkeztek a fórum törzsvendégeinél, és arra kérték őket, tanítsák meg őket a feltörésekre. Boa úgy döntött, először az érintkezés kultúrájára tanítja meg őket.

Erről így írt:

*Nyugodt körülmények között akarok dolgozni, anélkül, hogy mindenféle marhaság, különösképpen a nyilvánvaló, egyedülálló debilizmus elvonják a figyelmemet. Tehát: Nagyon kedvelem, ha valaki úgy köszön, hogy „jó napot", vagy „szia". Azt is elfogadom, ha valaki úgy köszön, hogy „szeva", de csak azoktól, akikkel régi, gyümölcsöző munkakapcsolatban vagyok. Mindenki mást kérek, tartózkodjanak az efféle bizalmaskodástól. Nem tűröm a tesó, csávó, kártyás srác megszólításokat.*

*Hajnali négy óra. Otthon vagy, a géped mellett, vagy a nőddel. Vagy Tolsztoj Háború és békéjét olvasod. Neked ez az élvezet hajnali négy órakor. Tehát el vagy foglalva. Kitartóan csengetnek. Kérdés: Te rögtön kitárod az ajtót anélkül, hogy kikukucskálnál, vagy ránéznél a kamera monitorjára, és mosolyogva betessékeled a csövest az ajtón? Töltesz neki sört, kikérdezed az életéről, meghallgatod a kéréseit, tehát ilyen idilli a kép? Vagy mégis csak megkérdezed (legalább azt, hogy): Ki az? Biztos megkérdezed, elsőre kulturáltan, hogy ki az a barom hajnali négykor, a franc vigye el, aki ilyenkor csenget? Senkit, a jó anyját sem vártad, csessze meg! Mi a francnak jönnek kötegszámra, se puszi, se pá, autorizációs kérések ICQ-n. Van ott egy kis ablak – „reason for authorization request", vagy valami hasonló. Egyáltalán nem nehéz egy sort bepötyögni, mondjuk, ez és ez vagyok, ez és ez a kérdésem. Más szóval, mondd meg a kémlelőn keresztül, hogy ki vagy, és miért jöttél.*

Amúgy Boa pontosan tudta, miről szól a Bolygó. „A dolog, hogy hogyan lopjunk amerikai hitelkártyaadatokat, Boával kezdődött – mesélte[32] később az egyik kártyás. – Ez a lelkes srác egész továbbképzéseket tartott a fórumokon: mindenkit az amerikai hitelkártyaadatok ellopására tanított. A CarderPlaneten sokan osztottak meg ilyen titkokat. Az orosz hekker nem mohó ember, nem holmi piti kiberzsebtolvaj, hanem értelmiségi, bizonyos skrupulusokkal. Oroszországból majdhogynem nyíltan ki lehet fosztani Amerikát, folytatva ezzel a hidegháború tradícióját és az FSZB etetését. 2002-ben annyi rés volt az online kifizetésekben, hogy ezeken keresztül vagonokkal lehetett volna szállítani a pénzt."

Boának voltak a CarderPlaneten kívüli projektjei is. Például a Fabriki nevű weboldala, a boafactory.net minden igénylőnek felajánlotta, hogy három nap alatt orosz állampolgársághoz juttatja, illetve hogy egy tekintélyes főiskola befejezéséről diplomát kaphat, vagy vízumhoz, vagy vezetői engedélyhez juthat. Itt gyakorlatilag bármilyen dokumentumot úgy hamisítottak, hogy azokat szinte



lehetetlen volt megkülönböztetni a valóditól. Az új, külföldre érvényes útleveleket még a semleges országokba való beutazásról, illetve az azokból való kiutazásról szóló pecsétekkel is ellátták, hogy az útlevél ne nézzen ki újnak. Ezen kívül a Boafactory hamis hitelkártyákhoz is juttatta az érdeklődőket. Azt beszélték,[33] hogy az „iroda" szolgáltatásaihoz ezrek folyamodtak.

2004-re a hitelkártyacsalás az orosz nyelvű felhasználók körében annyira tömegessé vált, hogy az angol nyelvű média „kiber-hidegháborúról" kezdett beszélni. Az év nyarán Script bejelentette, hogy kilép a CarderPlanetből, majd rövidesen az egyik adminisztrátor a fórumra kirakott egy posztot, amelyben közölte, a Bolygót „ideje bezárni", mivel azt mindenféle titkosszolgálat – az orosz és a külföldiek is – megfigyelés alatt tartja.

*Az FBI nyomozói az AOL* céghez szinte már hazajárnak, hogy megszerezzék az ICQ-s eseménynaplókat, és előzményeket kivonatait. Az FSZB emberei a tárhelyszolgáltatóknak pénzt kínáltak az ehhez a fórumhoz tartozó eseménynaplóért. Lehetünk bármennyire okosak, és bármennyi proxyt használunk is, lehet VPN-ünk a világ legtávolabbi zugában – mindannyian emberek vagyunk, emberi tényezőkkel. Tisztában vagyunk vele, hogy sokan elveszítik a munkájukat, sokan nem tudnak többet belépni, és társalogni az elvbarátaikkal. Viszont, sajnos, mi nem akarjuk tartani a seggünket mások keresetéért.*

A holmijaik összegyűjtése és a felhasználók kontaktjainak cseréje két hét alatt lezajlott. A CarderPlanet egyik tagja búcsúzóul verset írt a Pontok nevű rapegyüttes egyik dalának motívumaira: „Szomorúság tölti be a lelkemet, és sötét kenderfüst marja a szememet, mintha könnyek akarnának belőle kicsordulni. Emlékszem, valahányszor betértem ide, a feketéskék színt látva mintha újjászülettem volna."

* Az AOL az America Online rövidítése, amely egy céges hálózati szolgáltató és internetszolgáltató.

A fórumot bezárták, ennek ellenére hamar elkezdődött a résztvevők letartóztatása. Egy év alatt elértek Scriptig is, akiről kiderült, hogy nem más, mint a huszonkét éves Dmitrij Golubov. A letartóztatás pillanatában a nagymamája odesszai házában rejtőzködött. Golubovot nemzetközi bűnbanda létrehozásával vádolták, amely több mint tizenegymillió dollárt lopott. Tizenkét évnyi szabadságvesztéssel fenyegették, de végül a letartóztatás alól az ítélethozatalig felmentették[34] – ezt követően két parlamenti képviselő személyesen kezeskedett érte. „A fiatalemberek egyszerűen csak loptak – nyilatkozta egyikük. – Ő csak egy fiatal és tehetséges ember. Az ilyen gyerekek képezik a fiatalságunk krémjét." Az egyik hekkerfórumon Golubov szabadulását így kommentálták: „Miért is vagy te nekem olyan szép! ...és szárazon kijönni a vízből – erre nem mindenki képes!"

Golubov még csak meg sem jelent a bíróság előtt. Igen gyorsan ő maga is politikus lett, sőt megalapította Ukrajna Internetpártját. A legutóbbi elnökválasztáson a pártja megpróbált saját jelöltet állítani, Darth Alekszejevics Vader személyében, aki a *Csillagok háborúja* főgonoszának arcát használta. 2018-ban Golubov bitcoinmilliomossá vált.*

A CarderPlanet és elvtársainak sorsa különbözőképp alakult. Volt, aki úgy döntvén, hogy már elég pénze van, egyszerűen abbahagyta a lopást, és elhagyta Oroszországot. Egyikük azt mesélte nekem, hogy a legkedvezőbb időszakban a hitelkártyacsalásból havonta ötvenezer dollárra tett szert, de miután megkereste a pénzt a lakásra, a házra és a sportkocsira, a nyugalom mellett döntött, és egy ázsiai országban telepedett le. Más kártyások új felületeket hoztak létre, amelyeket most már bonyolultabb megfigyelni. A CarderPlanet kiberalvilágra gyakorolt hatásának jelentőségét talán a Russian Business Networkkel lehet összevetni, amelynek felvirágzása 2006–2007-re tehető.[35] A CarderPlanet néhány egykori tagja folytatja a szakmát, és manapság például – mintha egyáltalán nem is rejtőzködnének – a közösségi oldalakon nyílt társaságokat hoznak létre, ahol asszisztenseket keresnek maguknak, és videókat töltenek fel arról, hogyan veszik fel a lopott pénzt a bankautomatákból.

A legrosszabbul Script legsikeresebb bajtársai jártak. A titkosszolgálatok világszerte valósággal vadásztak rájuk, és egyesével fogták el őket.

* Lásd Fogalomtár.

*8. fejezet*

## A krími disszidens

Egy darab szalonna. Két üveg sós uborka. Egy vekni fekete kenyér. Egy bőrönd, benne egy pár futócipő és egy farmer. Julio Cortázar novellaskötete. A *Miselovka* (Egérfogó) nevű együttes albumának kazettája.

Mindezt a letartóztatásakor megtalálták és el is kobozták[36] a Krímből származó Roman Vegától: ő volt Sztyepanenko is, Boa is és Udav is. 2003 februárjában tartóztatták le Cipruson. A Bolygó másik egykori tagjának szavai szerint[37] Vegánál találtak még vagy kétszáz fényképet is a CarderPlanet tagjairól: folyamatosan gyártotta nekik a hamis útleveleket.

Roman Vega a Szimferopoli Állami Egyetem matematika szakán végzett, ezután a komplex védelem és hírszerzés rendszerének szakembereként dolgozott. Rajongott a hegymászásért, a barlangászásért, a rövidhullámú rádióállomásokért, valamint az olyan törvényellenes kalandokért, amelyekről még most is csak keveset tudni (és alapvetően azt is csak az ő szavai alapján). A hekker állítólag nemcsak iratokat, de fegyvereket is árult. 1993-ban Egyiptomban tartóztatták le, 1999-ben pedig Miamiban. „Az FBI igyekezett kreálni egy ügyet, amely szerint állítólag az egyik akkori miami társaságnak szándékában állt fegyvert és speciális technikai eszközöket szállítani a baszk harcosoknak a spanyolországi San Sebastianba – írta[38] Vega a blogjában. – Ezenkívül Kronstadtban van egy régi dízel-tengeralattjáró, amit fémhulladékként akartak eladni, ám az orosz haditengerészet tengeralattjárója papíron a Kolumbiából az Egyesült Államokba tartó ipari léptékű kokainszállítás



eszközévé változott." Vega így folytatta: „utána pedig Washington minden további nélkül rám akarta kenni, hogy elloptam kétszázötvenmillió dollárt, meg azzal gyanúsított, hogy nemzetközi hekker- és kártyás bandák állítólagos szervezője és vezetője voltam."

A ciprusi börtönben Vega másfél évet ült, ezt követően kiadták az Egyesült Államoknak, ahol körülbelül tíz éven át egyik városból a másikba dobálták, miközben nem emeltek ellene vádat: Vega volt San Franciscóban, Oklahomában, Atlantában, New Yorkban és Santa Barbarában. Az ítélet, amelyet végül csak 2013-ban, a letartóztatása után tíz évvel róttak ki rá, tizennyolc év börtön volt, tömeges feltörésekért és hekkerek százainak egyesítéséért.

Az USA-ban Vega részletes naplót vezet. Kézzel írt feljegyzéseit átadja a barátainak, akik ezeket a romanvega.ru weboldalon publikálják. Ahogy egykor a CarderPlanetre, Vega most is sokat ír, elég tehetségesen. A naplókból kiderül, hogy az amerikai börtönökben ácsként és asztalosként dolgozik egy bútorgyártó csapatban, valamint levelezőn elvégzett egy főiskolát Minnesotában. Vega hetente egy órát japánul tanul, dobol és heti kétszer zongoraórára jár, valamint franciát és spanyolt tanít, néhány naponta mezítláb fut a belső udvaron, és eközben a lepkéket számolja – a huszonegy kilométer futás alatt hetet számolt össze. A cellában öt könyvnél többet nem engednek tartani, de neki körülbelül félszáz van, ezért mindig azzal fenyegetik, hogy zárkába kerül. Az utóbbi néhány évben Vega próbált olyan iratokat előkészíteni, amelyek alapján átvihetik a büntetése hátralévő idejére Oroszországba, amelynek mostanra részévé vált az ő hazája, a Krím is.

Néhány feljegyzését Vega „a most folyó események krónikájának" nevezi, valószínűleg arra az ellenzéki jogvédő kiadványra utalva, amely a Szovjetunióban 1968 és 1984 között látott napvilágot. Olykor válaszol a weboldalát látogatók kérdéseire. Például, amikor azt kérdezték tőle, változtatna-e valamit az életén, ha tudná, hogy húsz évre

börtönbe fog kerülni, azt írta, „a fizikai börtönnél szörnyűbb a belső börtön, a lelki börtön". „Mi a jobb: élni teljes erővel, kipróbálni magamat ebben is és abban is, bátran elébe menni az új megtapasztalásának, a veszélyeknek és a kalandoknak, nem félve a nehézségektől, legyőzve a lehetőségeim határait, keresztülmenni megpróbáltatásokon, városokon és országokon, győzelmeken és vereségeken, szomorúságokon és örömökön – vagy pedig egész életen át húzni magunk után egy unalmassá vált munka igáját, vonszolni egy nyomorúságos létet, azzal az egyetlen gondolattal, hogy »bárcsak ne történne semmi«, nehogy összedőljön ez a szánalmas kis világ amiatt, mert a lelkem fél élni? Mi a jobb? Mindenkinek a magáé – írta Vega. – Emlékeznek O. Henryre? »Nem a kiválasztott útjainkban van a lényeg, hanem abban, hogy a bensőnk késztessen kiválasztani az útjainkat«."

2016 februárjában Vega börtönében megjelent egy új fogoly – Mihail Gorbacsov néven. Vega érdeklődött, és kiderült, hogy az egyik afroamerikait hívják így, aki elmondta, hogy az anyja gondolta ki neki ezt a nevet, amikor 1989-ben, a televízió előtt, az ajtófélfánál ülve, megpillantotta a képernyőn a szovjet főtitkárt, aki a peresztrojkáról beszélt. A börtönben a fekete bőrűeket Vega általában nem szerette: „hogyha az összes ilyesfélét itt szabadon bocsájtják, akkor az országra elkerülhetetlenül és gyorsan a teljes és végérvényes káosz, mészárlás és viszály köszönt, a normális embereket pedig (már aki túléli) mind térdre kényszerítik." Az egykori hekker, Dmitrij Naszkovec mesélte,[39] hogy Vega orosz patriótának tartja magát, és az Egyesült Államokat mindig is olyan ellenségnek tekintette, amelyet „meg kell fojtani".

Az amerikai börtönrendszer Vega kedvenc témája: tudja, hogy az Egyesült Államokban van a legtöbb fogvatartott az egész világon, és előszeretettel citálja Adam Gopnik a *The New Yorker* című lapban ezzel a témával foglalkozó cikkeit. Amikor 2011-ben a börtönben Vegá levelet kapott Barack Obama választási stábjától azzal a kéréssel, hogy támogassa Obamát az újraválasztási kampányában (ez egy bevett szavazatgyűjtő gyakorlat az USA-ban), a hekker egy felháborodott, hatoldalas, a rabmunkáról és az igazságtalanságról szóló levélben[40] válaszolt:

*Az Amerikai Egyesült Államok elvette tőlem a szabadságot, a napot (amit néhány havonta csak egyszer láthatunk a börtönautóbusz ablakából, a bíróság felé vezető úton), az igazságszolgáltatást. Annak a lehetőségétől is megfosztottak, hogy láthassam az anyámat – állandóan megtagadják tőle a vízumot az önök dicsőséges amerikai követségén. A határ lakatra van zárva. A hetvenéves anyám így sehogy se tud találkozni a fiával, akit egy évtizede ítélet nélkül tartanak fogva. A te országod elvette az egészségemet, sőt, még a fogaimat is.*

Vega gyakran emlegeti Szolzsenyicinnek *A Gulag szigetvilágát*, különösen, amikor azokról az alaptalan eljárásokról beszél, amelyek véleménye szerint az amerikai oroszok ellen folynak. Múltbéli hekker önmagáról, aki valaha Boának nevezte magát, a naplókban szinte nem is tesz említést.

*9. fejezet*

## A fehérorosz Ali Baba

2004-ben a fehérorosz Szergej Pavlovics, a CarderPlanet weboldal egykori törzsvendége vett magának egy új Mercedest, és a 999-es számot függesztette rá. Aztán megünnepelte a DumpsMarket, saját hitelkártyacsalós weboldala születésnapját. A mulatság, amelyre a FÁK* hekkereinek nagy többsége hivatalos volt a dácsán,** négy napig tartott. „Az alkohol úgy folyt, mint a folyó, a szajhák az asztalokon táncoltak, azok a gazfickók meg szívták a kokaint" – emlékezett vissza Pavlovics. A vendégek szórakoztak, miközben pisztolyokkal az üvegekre lövöldöztek, a szakácsok meg egyenesen a tóból fogták ki a pontyokat és a tokhalakat, aztán a grillen megsütötték őket.

Nem sokkal ezután Pavlovics vendégségbe indult a barátnőjéhez. Őt követve a rendőrség is megérkezett.

A rendőrök házkutatást tartottak, ezalatt a barátnője odaszólt Pavlovicshoz: „Nyulacskám, figyelj, hallgass rám! Nem tudjuk, mi fog történni veled. Egyet tehetsz, eszel egy keveset. Ki tudja, mikor lesz erre lehetőséged legközelebb." A barátnő piláfot és saslikot tett elé, a zakója zsebébe pedig

* A Független Államok Közössége a Szovjetunió felbomlási folyamatának végén, a szovjet utódállamok egy részéből alakult meg 1991 decemberében. Tagjai közé ma Azerbajdzsán, Örményország, Fehéroroszország, Kazahsztán, Kirgizisztán, Moldova, Oroszország, Tádzsikisztán és Üzbegisztán tartozik.

** A dácsa hétvégi házat jelent, ma gyakran a moszkvai agglomerációhoz tartozó lakóépületeket is így nevezik. – *A fordító megjegyzése.*



kenyérdarabot rejtett. Pavlovicsot bevitték a rendőrségre, és nem sokkal később a fehérorosz bíróság hat év börtönre ítélte hitelkártyacsalásért.

A börtönben írta meg a *Hogyan loptam milliókat. Egy bűnbánó kártyás vallomása* című memoárját, amelyben részletesen beszámol arról, miért és hogyan vált hekkerré. A memoár tele van szomorúsággal és költői gondolatokkal. „A feleségem, több mint valószínű, el fog hagyni. A nagyapám, aki engem felnevelt, meg fog halni [mire kijövök a börtönből] – írta Pavlovics. – Az anyám megöregszik – sokkal inkább a bánattól, mint az életkoránál fogva. A barátaim számára fantommá válok, akivel nem lesz majd miről beszélni."

Pavlovics meg van róla győződve, hogy a szegénység és a családon belüli problémák miatt vált hekkerré: „Kiberbűnözővé (a volt Szovjetunió területén) leginkább a pénztelenség miatt válnak az emberek. Elég eszük van, de önmagukat mégis csak a bűnözésben voltak képesek megvalósítani." Pavlovicséknak akkor lett számítógépük, amikor ő tizenkét éves volt, s a barátai többnyire akkor még a Dendyhez hasonló konzolon játszottak. Ennek ellenére a fiú a szabadideje meghatározó részét a számítógépes klubban töltötte: otthon nem akaródzott lennie, mert az anyja ivászatokat rendezett ismeretlen férfiakkal. Pavlovics a *Counter-Strike*-kal és a *Heroes of Might and Magic III*-vel játszott, amikor egyszer csak az ütközetek közötti szünetben ráakadt a CarderPlanetre.

Mivel először volt a weboldalon, úgy érezte magát, mint „Ali Baba, aki rábukkant egy kincsekkel teli barlangra". A kamasz felfogta: megtalálta a könnyű meggazdagodás módját anélkül, hogy fel kellene állnia a számítógép mellől. Míg egy átlagos munkáért körülbelül kétszáz dollárt kaphatott volna havonta, addig a hitelkártyás csalók utasításainak teljesítése milliókat ígért. Regisztrált a fórumra, és egy kis idő múlva létrehozta a sajátját: a DumpsMarketet,

az ellopott hitelkártyaadatok és a hamis dokumentumok viszonteladási piacát. Az úgynevezett dumpokat* más hekkerektől kapta, vagy áruba bocsátotta azt, amit ő maga lopott el.

Pavlovics és a Bolygó más hekkerei is jobbnak tartották, ha kizárólag külföldiektől lopnak. „Szánalmas volt [a volt Szovjetunió területének célpontjaira támadni] – magyarázta. – Amerikában minden bankszámla biztosított, nálunk viszont a kártyatulajdonosokat a rendőrségre hurcolják, mindenki gyanússá válik, hogy saját magától lopott, s azt most még vissza is akarja szerezni. Erre a mi évszázadunkra elég a burzsujokból is. Patriotizmust tanúsítunk, nemdebár. A hidegháború folytatódik, most új fordulatot vett, csak épp a kibertérben." Pavlovics beismerte,[41] hogy „soha nem lenne képes arra, hogy tömegközlekedve a pénztárcákból lopjon", de az interneten „nem érzed azt a határt, amelyen túl már a bűnözés kezdődik". Azt is mondta, hogy „jóval egyszerűbb egy kiválasztott rendszert feltörni, mint egy bankot". A pénzt Pavlovics készpénzben tartotta egy bőröndben, amit a nagyapja kertjében ásott el.

„Teljesen a munkának szenteltem magam, elszívtam két doboz erős Marlborót naponta, felszedtem tíz felesleges kilót, a tevékenységem speciális jellege pedig nem igazán tette lehetővé, hogy buzgón új barátokat keressek – mesélte Pavlovics. – Nincs azon mit csodálkozni, hogy akkoriban alapvetően drága kurvákkal háltam, a magas jövedelmem révén a legjobbak lettek az enyéim. Milliókkal az élet különlegesebb, fényesebb, boldogabb. Olykor kontár módon, olykor nagyon is okosan költöttem a pénzt. Megválni a pénztől nőkkel lehet a legszebben. De a legkellemesebb, és bizonyára a leghelyesebb, ha Mikulás leszel, és megmented súlyosan beteg emberek életét az-

* Lásd *Fogalomtár.*



zal, hogy kifizeted a műtétjüket. Az anyámnak új autót, az unokaöcsémnek számítógépet és rollert vettem, a barátnőm anyjának kifizettem egy tengeri körutat, hogy ne mondjam, még a volt barátnőm anyjának is." Amikor egyszer Pavlovics elhatározta, hogy személyesen is megismerkedik más hekkerekkel, azok a találkozóra két pornószínésznőt is meghívtak.

Egy alkalommal Pavlovicstól a WebMoney-n tárolt számlájáról körülbelül tízezer dollárt loptak el. Amikor megtudta a tolvaj IP-címét, az FSZB általa ismert embereinek körülbelül háromszáz dollárt fizetett, hogy megtudja a tolvaj otthoni címét is. Kiderült, hogy oda egy nyugdíjas van bejelentve a tizenkét éves unokájával. Pavlovics békén hagyta őket.

A börtönből Pavlovicsot idő előtt kiengedték, 2007-ben. Szinte azonnal visszatért a hitelkártyacsaláshoz, a fegyverek árusításához és a pornóoldalak létrehozásához, de ezzel párhuzamosan konzultált a helyi titkosszolgálatokkal: azok a kiberbűnözés elleni harc hivatalvezető-helyettesét azzal gyanúsították, hogy ő maga is kártyássá vált. A börtön után Pavlovics aktívan sportolni kezdett, az ismerősöket összekötő Mamba nevű közösségi oldalra is regisztrált, és az is eszébe jutott, hogy saját vodkákat dob piacra Hacker & Carder néven, mivel úgy látta, a vodka „ideális marketingtermék". Végül a projekt nem jött össze: „Az idő nagy része nők hajkurászására ment el."

2009-ben Pavlovicsot ismét letartóztatták. Ez alkalommal a bíróság tíz év börtönre ítélte adatlopásért és hamis bankkártyák értékesítéséért. Ugyanekkor az amerikai titkosszolgálatok is felkutatták: Pavlovicsot annak a csoportosulásnak a tagjai közé sorolták, amely a legnagyobb lopást hajtotta végre[42] az Egyesült Államok történetében – ez körülbelül százmillió hitel- és bankkártyát érintett.

Amerikának nem adták ki Pavlovicsot. „Hogyha ott ítélték volna el, akkor mindenképp életfogytiglani bör-

tönbüntetés nézett volna ki számára. Úgyhogy megint szerencséje volt, hogy mi tartóztattuk le, nem pedig ők" – mondta 2009-ben a fehérorosz KGB „K" ügyosztályának parancsnoka, Igor Csernyenko. Másodjára Pavlovics 2015-ben szabadult a börtönből, és elindította a Carding Pro nevű weboldalt, amelyen a feltörésekre vonatkozó folyamatleírásokat és más cikkeket tesz közzé. Pavlovics többek között a saját bizniszére vonatkozó terveiről is nyilatkozott:[43] arra készül, hogy létrehozza a Hacker & Carder vodkamárkát.

*10. fejezet*

## A teslás kalandor

2010 augusztus elején Vladiszlav Horohorin a nizzai repülőtér várótermében ücsörgött, egy koktél társaságában.[44] Monacóban töltött szabadságáról tért haza. Ebben a pillanatban automata fegyverrel felszerelt maszkos szpecnazosok* törtek be az épületbe.

A rendőrség 2003 óta kereste Horohorint a legkülönbözőbb országokban; azóta, hogy saját magát BadB-nek nevezte, és utolsóként maradt szabadlábon a CarderPlanet egykori vezetői közül.

Horohorin szülei akkor váltak el, amikor még kicsi volt, gyermekkorát az anyjával töltötte. A pénz nem volt elég – még megfelelően gyors internetre sem. Ekkor Horohorin feltörte az internetszolgáltató védelmi rendszerét. Amikor lefülelték, a szolgáltató tulajdonosai nem a rendőrséghez, hanem – ahogy az a kilencvenes években megszokott volt – a bűnbandákhoz fordultak. A kamasz srác megúszta némi ráijesztéssel, de anyjával azért hamarosan Izraelbe költöztek. Ott Horohorin bevonult a seregbe, és most már ennek az adatbázisát törte fel, hogy gyakrabban mehessen eltávra. Ismét lefülelték – és ismét megúszta komolyabb következmények nélkül. Ugyanebben az évben Horohorin összeismerkedett a CarderPlanet alapítójával, a hekker Scripttel, tőle kért egy lopott kártyát, hogy ebből fizesse a hozzáférést a pornóoldalakhoz. Hamarosan mindketten

* Szpecnaz: különleges rendeltetésű alakulat, kommandó. – *A fordító megjegyzése.*

a világ hitelkártyás csalóinak legsikeresebbjei közé tartoztak.

Horohorin egyik ismerőse „elvtelennek és hazárdjátékosnak" nevezte őt. „Nagyvilági kalandor. A legkedveltebb mondása a *Lopni csakis milliókat, hálni csakis királynővel* volt – mesélte[45] az egyik carderplanetes harcostársa. – Bizonyos időközönként egyáltalán nem volt pénze, mert folyamatosan rulettre, ivászatra, kurvákra költötte."

Szerette a látványos gesztusokat. Egyszer Horohorin és Pavlovics éjszakai klubba ment, és ott „kibérelték" az összes sztriptíztáncosnőt. A hekker rajongott a jachtokért, a drága autókért, és nem sokkal a letartóztatása előtt megvette magának az első Teslák egyikét. Volt rá pénze: épp a Royal Bank of Scotlandot törték fel, és társaikkal majdnem tízmillió dollárt kerestek.

Horohorin azt követően sem hagyott fel a hitelkártyacsalással, hogy a CarderPlanetet bezárták, de a biznisz érdekében nemsokára hazafias szimbólumokat kezdett használni, és Vlagyimir Putyin portréit. 2007-ben az egyik hekkerfórumra kiposztolt egy reklámnak szánt hirdetést, amelyben azt ecsetelte, hogyan kereskednek az ellopott kártyák adatbázisával immár körülbelül nyolc éve. Illusztrációként mellékelt egy kis rajzot is, amelyen Vlagyimir Putyin érdemérmet nyújt át a hekkereknek, a képaláírás pedig így szólt: „Várjuk önöket, hogy megküzdjünk az USA imperializmusával. Így fektetjük be az USA pénzét az orosz gazdaságba, elősegítve a növekedést."

2007-ben Horohorin egy kétrészes animációs filmet készített,[46] amely a hekkereket az Egyesült Államok elleni támadásra szólította fel. Ebben egy hekker usánkában és trikóban adja át az adatokat egy másik kiberbűnözőnek, az pedig készpénzre váltja a hitelkártyákat. Ezt követően az akkori amerikai külügyminiszternek, Condoleezza Rice-nak kiesik a szeme, az ifjabb George Bush főbe lövi magát, mert a Fehér Házból az összes pénz eltűnt. A film végén a rajzolt Putyin a hekkereket kitünteti a Kremlben.



Miután a nizzai repülőtéren letartóztatták, Horohorin két évet töltött francia börtönben, az USA-ba történő kiadatására várva. Ez alatt értékesítette a vagyontárgyait: az izraeli házát, amely körülbelül egymillió dollárt ért, a franciaországi villáját, amely pedig hárommillió eurót. Amerikában vádalkut kötött, és átadta a hatóságoknak a többi hekkerrel folytatott levelezését. Felszólították, hogy tegyen vallomást Roman Szeleznyov ellen – ő szerepelt a CarderPlaneten pSzih álnéven. Horohorin azt állítja, visszautasította, hogy az FBI ügynökeinek jelentsen: „Fiúk, mi együtt lógtunk a fürdőben. Miféle vallomás? Menjenek a ..."

Hét év börtönt kapott, de amikor idő előtt szabadon bocsátották, Izraelnek adták ki. Az orosz állami tévécsatornánál, ahová interjúra hívták be, a hekker azt mesélte,[47] hogy amíg fogva tartották, résekre bukkant az amerikai katonai szervezetek védelmén. Ezután kijelentette, az az álma, hogy az orosz titkosszolgálatoknál dolgozzon. „Az orosz hekkerek üldözni fognak, de ez boszorkányüldözés, ők maguk kreálnak ellenséget maguknak – jelentette ki Horohorin. – Loptam, de nem az emberektől, hanem az amerikai államtól. Tőlük muszáj lopni. Ők az egész világtól lopnak." E közlemény megjelenése után pár hónappal a hekker Oroszországban kezdett utazgatni.

Jelenleg Horohorin a saját Facebook-profilján olyan nosztalgikus fotókat posztol, amelyeket a letartóztatása előtt készített, illetve filozófiai okfejtéseket tesz közzé az életről. „Harmincöt éves vagyok – írja. – Egy zseniálisan tehetséges idióta, aki nyolc nyelven beszél, és bejárta a világot. Néha úgy érzem, szeretném megváltoztatni a világot. De hogy tudnám megváltoztatni a világot, hogyha önmagamat sem tudom megváltoztatni? Nem is oly rég, a világ túloldalán rég nem látott ismerőseimmel találkoztam újra. Szép és okos feleségük van, az egyikőjüknek két csodálatos gyereke. Megváltoztak, szeretnek és szeretik őket – én pedig őket, akikre én emlékeztem, már nem ismerem. Én viszont semmit se változtam. Ezért ma is úgy ismét-

lem, mint egy mantrát: »Uram, adj türelmet, elfogadni azt, amin nem tudok változtatni, és bátorságot, megváltoztatni azt, amit tudok. És adj bölcsességet, hogy meg tudjam különböztetni az egyiket a másiktól.«"

És mint oly sok orosz hekker, Horohorin is ír verseket:

*De kik vagytok ti most?*
*A Facebook és Lady Gaga generációja*
*Ahol a lájkok mennyisége számít*
*És a barátok minőségét értékelitek*
*Vagy ráöntve a haragotokat körülöttetek mindenre*
*és mindenkire, virtuálisak maradtok*
*És az öröm?*
*Az avatár mögött csak nyomai látszanak*
*az álmatlan éjszakáknak*
*A szem felduzzad a szomorú gondolatoktól*
*és a könnyektől*
*A nickname-ért komplex védelem jár*
*De kit rejtegetsz a lelkedben, az én örömömet?*
*Arra, amit keresel – ott nem találsz se választ,*
*Se segítséget, se bölcs tanácsot*
*Annál is kevesebbet, mint amiről valójában álmodsz:*
*Ott csak az agyrém megabájtjait és válasz nélkül*
*maradt kérdéseket leled*

*11. fejezet*

## pSzih

Mielőtt az amerikai bíróság ítéletet hozott volna az ügyében, Roman Szeleznyov hekker kézzel megírt angolul egy tizenegy oldalas szöveget. A következőket ecsetelte benne:[48]

*Vlagyivosztokban születtem 1984. július 23-án. Kétéves voltam, amikor a szüleim elváltak. Anyámmal egy másokkal közösen használt lakás szobájában éltünk, tíz négyzetméteren. Másik négy családdal laktunk együtt ezekben a nehéz időkben. Amikor hétéves voltam, az anyám vett egy lakást a bátyjától. Nem fizette ki a teljes összeget, ezért még egy éven át törlesztenie kellett. Szerényen éltünk, fájdalmas volt látni, hogy a mamának mindennap szenvednie kell. Pénztárosként dolgozott a kerület egyik boltjában, én az idő nagy részét egyedül töltöttem otthon. Így – önállóan – kezdtem tanulmányozni a számítógéptechnológiát. Kiderült, hogy jók a képességeim. Amikor az iskolában tanultam, felfogtam, hogy valahogy segítenem kell a mamának. Tizenhat évesen főiskolára mentem, ahol matematikát és informatikát tanultam. Jobbá akartam tenni az anyám életét, és azt akartam érezni, hogy ha lenne apám, büszke lenne rám.*

*Észrevettem, hogy az anyám gyakran iszik. Néha hét napon keresztül egyfolytában. Amikor tizenhét éves voltam, a mama meghalt. Amikor hazamentem az iskolából, a fürdőkádba fulladva találtam. Alkoholmérgezésben halt meg. A következő napon a bátyja elkobozta a lakásból anyám összes ékszerét és jó cuccát, nekem pedig azt mondta, hogy menjek el. Azt mondta, hogy a mama nem is fizette ki neki a lakást, pedig fizetett.*

*A temetés után többet nem mentem iskolába. Elkezdtem munkát keresni. Időnként a nagymamám segített.*

*Találtam munkát az egyik helyi számítógépes klubban. Huszonnégy órás szolgálatot ajánlottak. Körülbelül öt dollárt fizettek egy napért. Hamar rájöttem, hogy egyszerűen kihasználnak. Megpróbáltam az interneten munkát találni. Ez oda vezetett, hogy lejtőre kerültem. Bűncselekményekbe keveredtem. De nem a jó utat választottam: inkább hekkerré váltam, elkezdtem számítógépeket feltörni, hitelkártyákat lopni és más egyéb olyan információt, amit el lehetett adni. Ez a pénz elég volt. 2007-ben egy hatalmas hitelkártya-adatbázisra bukkantam, és ezt sok pénzért adtam el. Mohó lettem.*

*2008-ban feleségül vettem Szvetlánát. A következő évben megszületett a mi csodálatos Jevánk. Elutaztak pihenni. Én otthon maradtam. Ekkor váratlanul rablók törtek be a lakásba. Megvertek, megtudták a jelszavaimat, és elkobozták a számítógépeimet. Tudták, hogy mivel foglalkozom, és tisztában voltak vele, hogy nem fogják őket elkapni. Nem szenvedtem az anyagi veszteség miatt, de ismét pénz nélkül maradtam. Viszont tudtam, hogy hol szerezzek. Féltem, hogy a rablók visszajönnek, ezért a biztonságunk érdekében elutaztunk Balira.*

*2010 közepétől problémáim adódtak a munkával, semmilyen helyet se találtam. Ezért ismét azzal kezdtem foglalkozni, amihez értettem. Ekkoriban halt meg a nagymamám, aki az én igazi szülőm volt. Ő nem ismerte a rossz oldalamat, azt gondolta, hogy egyszerűen egy számítógép-specialista vagyok.*

*[A következő néhány mondatot a cenzúra kitörölte. Szeleznyov apjáról, Valerijről lehetett benne szó, aki az LDPR* színeiben az állami duma képviselője.] Apám meghívott a családommal Marokkóba. Egy nappal őelőtte érkeztünk meg. Elhatároztuk, hogy megreggelizünk egy hotelben, de ott azt mondták, csak akkor engednek be, ha zakót viselek. Zakóm nem volt, ezért átmentünk a legközelebbi kávézóba. A pincér azt mondta, hogy körülbelül fél órát kell várnunk. Hozzátette: „Ez rossz ötlet." De én nem értettem, mire gondol.*

* Az LDPR Oroszország Liberális Demokrata Pártjának rövidítése.



*A pincér kihozta nekünk az ananászlevet, és ugyanebben a pillanatban egy sahid felrobbantotta magát. Az egész kávézó a levegőbe repült,[49] mindenütt halottak és vér volt. A robbanástól súlyosan megsérült a fél fejem. Hál' istennek, a feleségemnek nem esett baja. [2011. április 29-én terroristák egy marrákesi kávézóban otthagytak két robbanószerrel teli aktatáskát, amelyeket mobiltelefonon keresztül robbantottak fel. Tizenhét ember halt meg. A marrákesi hatóságok a terrortámadásért az Al-Kaidát vádolták, de a szervezet megtagadta, hogy magára vállalja a robbantásért a felelősséget. – A szerző megjegyzése.]*

*Én nagyon rossz állapotban voltam, azt hittem, ott fogok meghalni. A feleségemnek azt mondták az orvosok, hogy semmit se tudnak tenni az életem megmentése érdekében. Egy bonyolult agyműtétre lett volna szükségem, amit nem tudtak megcsinálni.*

*Az apám valahogy megszervezte, hogy repülővel átszállítsanak Moszkvába. Az orvosok azt mondták az apámnak és a feleségemnek, hogy hamarosan meg fogok halni, de ha mégis csoda történne, akkor is „egész életemre zöldség maradok". A feleségem elhagyott, és elrepült a szülővárosába, mert azt gondolta, meg fogok halni.*

*Nem voltam megkeresztelve. Oroszországban az embereket a haláluk előtt meg kell keresztelni, különben pokolra jutnak. A kórházhoz tartozott egy pap, aki az apám kérésére gyorsan megkeresztelt. De csoda történt. Két hónap múlva felébredtem a kómából. Nem tudtam beszélni és járni, de értettem a beszédet és együtt tudtam működni. Három hónap múlva járni tudtam, egy év múlva helyreállt a beszédem és a felfogásom. 2011 májusától 2012 végéig különböző kórházakban voltam. Egyik operáció követte a másikat: az agyamon, a nyakamon. 2012 közepén elváltunk a feleségemmel. Azt mondta, azért hagyott el, mert nem akart egy „zöldségről" gondoskodni. Az USA-ba utazott a lányunkkal, magával vitte az összes pénzt.*

*2013-ban ismét elkezdtem számítógépeket feltörni és hitelkártyaadatokat árulni. Az életem szörnyű volt. Utáltam azt a férfit, aki a tükörből nézett vissza rám. Azt kérdeztem az Is-*

*tentől: „Miért mentettél meg engem?" Hamarosan azonban találkoztam Annával, aki a menyasszonyom lett. Vár engem Oroszországban. Szeret engem, és támogat immár három éve. Van egy lánya, akit örökbe akarok fogadni.*

*2014-ben az amerikai hatóságok letartóztattak. Amikor bekerültem a börtönbe, rossz volt az angolom. Megijedtem, összezavarodtam, a felét se értettem annak, hogy mi történik, és mit mondanak nekem az emberek. Az ügyvédem azt a borzalmas tanácsot adta, hogy harcoljak, különben életfogytiglanit fogok kapni. Most már világos, hogy minden egyes ügyvédnek, akivel csak dolgom volt, kizárólag a publicitás kellett.*

*Azt gondolom, ez az ár mindazért, amit az életemben elkövettem. Sok rossz cselekedetet hajtottam végre, és most kell vállalnom a felelősséget ezekért. Nem vagyok idealista. Felelni fogok ezért, mint egy férfi.*

*Meghallgattam azokat, akiket kiraboltam. Sírni szerettem volna. Voltak, akik miattam mentek üzletileg tönkre.*

*Félek a büntetéstől. De megértem, hogy nem csak financiális problémákat okoztam. Emberek veszítették el miattam a biztonságérzetüket – saját magukat, a pénzüket, az információikat.*

*Én, Roman Szeleznyov, azt szeretném mondani: „Nem volt igazam, sajnálom."*

*Remélem, hogy egyszer kijövök a börtönből. Dolgozni fogok, hogy kifizessem azt a pénzt, amit az áldozataim elvesztettek. Tisztességesen fogok dolgozni. A börtönben töltött évek alatt szereztem néhány szakképesítést – például vendéglátó-ipari és hotelmenedzsmentet tanultam.*

*A letartóztatásomig lefelé száguldottam egy halálosan veszélyes úton.*

*Nagyon szépen köszönöm.*

Ahogyan azt Szeleznyov periratai[50] mutatják, amikor tizennyolc éves volt, a programozás iránti rajongásról áttért az első feltörésekre. Ezeket pSzih néven követte el. Ezt a nevet használta akkor is, amikor regisztrált a Carder-Planethez hasonló hitelkártyacsalós fórumokra. Kezdetben adatbázisokat tört fel, hogy dokumentumokat lopjon



el (neveket, születési dátumokat, útlevél- és társadalombiztosítási adatokat), aztán lopni kezdte a hitelkártyák adatait is, és más kártyások adatbázisait is kezdte eladogatni.

Szeleznyov nem önálló számlákat tört fel, hanem amerikai kisvállalatok pénzforgalmi rendszereit, amelyeken keresztül e vállalkozások összes pénzügyi művelete folyt. Másokhoz képest gyakrabban váltak nála célponttá a washingtoni és más amerikai városok kis falatozói. A periratokban említést tesznek jó néhány pizzériáról és pékségről (mindez körülbelül 3700 kisvállalatot tett ki az összesen). Szeleznyov a kisvállalkozásokat a hibás védelmi rendszer alapján választotta ki: ezek a cégek nem rendelkeznek saját kibervédelmi ügyosztállyal, és általában rossz jelszavakat használnak. E megközelítés révén 2000-re Szeleznyov vált az egyik legsikeresebb kártyássá a világon.

Az USA titkosszolgálatai már 2005-ben vizsgálni kezdték Szeleznyov tevékenységét. 2009 májusában az FBI ügynökei Moszkvában találkoztak az FSZB képviselőivel. Az oroszok bizonyítékokkal szolgáltak az amerikaiaknak arról, hogy a pSzih álnév alatt a vlagyivosztoki illetőségű Roman Szeleznyov rejlik. Egy hónappal később, 2006 júniusában pSzih közölte a fórumon, hogy kiszáll a bizniszből, ezt követően a profiljait meg is semmisítette. Az Egyesült Államokban úgy vélik, éppen az FSZB adta át Szeleznyovnak az információt, hogy érdeklődnek iránta az amerikai hatóságok. A hekker levelezése azt támasztja alá, hogy Szeleznyov kapcsolatban állt az FSZB-vel. Szeleznyov egyik bűntársa azt fejtegette, hogy az FSZB információbiztonsági központjából fedezték Szeleznyovot. Még azt is mondta, hogy az FSZB tudja, ki Szeleznyov, és mivel foglalkozik.

A hírforrásom, akinek kibervédelemmel kapcsolatos a munkája, megerősíti, hogy azokat az orosz hekkereket, akik külföldi rendszereket törnek fel, szinte soha nem büntetik meg – az sokkal gyakoribb, hogy bevonják őket az állam javára végzett munkába. Minden orosz hekker ismeri a „ne dolgozz a .ru területén" kezdetű szöveget; vagy-

is tudja, hogy Oroszországban tartózkodva tilos az orosz bankok és cégek elleni támadás.

Miután megsemmisítette korábbi álnevét, Szeleznyov hamarosan mint Track2 és mint Bulba kezdett tevékenykedni. Csakhamar új szintre emelte bizniszét. 2009 szeptemberében megnyitotta az ellopott kártyaadatok webáruházát. Ez szinte teljesen úgy nézett ki, mint az Amazon: kategóriák szerint lehetett keresni és választani a különféle kártyatípusok és hitelintézmények közül. Az USA hatóságai úgy értékelték, Szeleznyov újragondolta a hitelkártyás piacot: korábban az ellopott kártyák a fórumok önálló ágain jelentek meg, most azonban az ellopott adatok cseréjének folyamatát optimalizálta és automatizálta. 2011 áprilisában Szeleznyov üzletében körülbelül egymillió új kártya jelent meg. Ezután néhány héttel Szeleznyov elutazott Marokkóba, és majdnem meghalt a robbantás következtében. Amíg az orosz férfi lábadozott, bűntársai folytatták a projektet, de végül 2012 januárjában a weboldalt bezárták.

Amikor kijött a kórházból, Szeleznyov felvette a 2Pac álnevet. Alapított még egy webáruházat, és beindította azt az oldalt, amelyen alapvető instrukciókat lehetett találni arról, hogyan kell ellopni a banki adatokat, és miként kell felhasználni azokat. A weboldal felső részén angolul állt egy közlemény: *„Most megtudhatja, hogyan kell pénzt keresni. 500 dollártól 5000-ig, sőt 50 000-ig. Jusson eszébe, hogy ez illegális út! Az egész folyamat az, az elejétől a végéig."* A weboldal működése első hónapjában, 2014 júniusában, három és fél millió látogatója volt.

Szeleznyov nagyon sok pénzt keresett. Közismert,[51] hogy csak az egyik szolgáltatón keresztül történő átutalásért körülbelül tizennyolcmillió dollárt kapott. Vagyona pontos mérete ismeretlen: a hekker a Bitcoinon, a WebMoney-n és más elektronikus pénztárcákon keresztül kapta a pénzt. Két házat vett Balin, gyakran fényképezett bankjegykötegeket és drága autókat. Van egy fotó, amelyen a Vaszilij Blazsennij-székesegyház előtt egy sportautó mellett áll,



amely majdnem ugyanolyan, mint a másik letartóztatott orosz hekkeré, Jevgenyij Nyikuliné.[52] (Őt Prágában tartóztatták le 2016 októberében, s azzal vádolták, hogy feltörte a LinkedInt, a Dropboxot és egyéb szolgáltatásokat. Nyikulin azt állította, hogy azt követelték tőle: ismerje be, hogy ő törte fel Hillary Clinton postafiókját Vlagyimir Putyin parancsára.)

Mivel tisztában volt vele, hogy az FBI ügynökei megfigyelés alatt tartják, Szeleznyov folyamatosan utazgatott. Azokat az országokat választotta ki, amelyekben nincs kiadatás az Egyesült Államokba, és csak az utolsó pillanatban vette meg a jegyeket, hogy megzavarja a titkosszolgálatokat, nehogy követni tudják a helyváltoztatásait.

2014 júliusában a Maldív-szigetekre repült, ahol napi 1400 dollárért vett ki egy villát. „A legdrágább villát vettem ki magamnak, és saját szolgám van" – írta az egyik bűntársának.

Miután megtudták, hogy Szeleznyov a Maldív-szigeteken tartózkodik, az FBI ügynökei kérvényezték az amerikai külügyminisztériumnál, hogy vegyék fel a kapcsolatot a helyi hatóságokkal. Az egyeztetéseket követően az országok rendőrfőnökei mgállapodtak a hekker letartóztatását illetően, a kiadatásról szóló egyezmény hiánya ellenére. A Bloomberg cikke szerint a Maldív-szigetekre az FBI hawaii irodájából érkezett két ügynök. Ők a rendőrséggel együtt követték Szeleznyov helyváltoztatásait. Amikor a repülőtérre ment, ahonnan Moszkvába repült volna, letartóztatták. A hekkert beültették egy magánrepülőgépbe, és tizenkét óra alatt átszállították Guamba, egy amerikai katonai bázisra.

A periratok adatai alapján Szeleznyovnál volt egy notebook, benne 1,7 millió ellopott hitelkártya adataival, sőt a szerverekre vonatkozó jelszavakkal, e-mail-fiókokkal és pénzügyi átutalások nyomaival.

Amikor Guam után Seattle-be került, Szeleznyov azt nyilatkozta, hogy az FBI ügynökei megverték, de a bíróság

ezt a vádat visszautasította. Az orosz külügyminisztérium a férfi letartóztatását emberrablásnak, illetve „Washington újabb barátságtalan lépésének" nevezte. Szeleznyov apja indítványozta,[53] hogy a Maldív-szigetek ellen léptessenek életbe gazdasági szankciókat. Azt mondta,[54] Romant nyolc páncélozott autón szállítják, egyikből a másikba ültetve – „ezzel valamiféle internetes bin Ládent csinálnak belőle".

Szeleznyov letartóztatását követően egy hónappal a 2Pac fórumán közlemény jelent meg: „Elnézést kérünk, hogy nem frissítjük a fórumunkat. A főnök autóbalesetet szenvedett, kórházban van."

Az ügyész azt nyilatkozta,[55] hogy Szeleznyov az összes, valaha is bíróság előtt álló kiberbűnöző közül a legkomolyabb. A vád rendkívüli számítógépes képességekkel rendelkező embernek nevezte, aki néhányszor azért tért vissza a kiberbűnözéshez, hogy „növelje a támadás léptékét".

A működésével okozott kárt százhetvenmillió dollárra becsülték. Az ügyész az orosz férfit még Tony Sopranóhoz, a *Maffiózók* című sorozat főhőséhez is hasonlította.

„Szeleznyov letartóztatása ritka győzelem a kelet-európai kiberbűnözés ellen folytatott harcban – jelentették ki az amerikai ügyészek. – Sok hekker él Oroszországban, akit nem adnak ki bűnözőként az USA-ba. Hogyha Szeleznyovot kiadjuk az oroszoknak, számításba véve az orosz bűnüldöző szervezetekkel fenntartott kapcsolatait, otthon büntetlenül tevékenykedhet tovább."

Szeleznyov sokáig megtagadta az együttműködést a vizsgálattal, és elhúzta az eljárást. Fogva tartása idején rejtjelezett telefonbeszélgetéseket folytatott a börtönből az apjával. Ezek során „Andrej nagybácsi verziójáról" egyeztettek, azaz a tárgyalás elhúzásáról, ami alatt Szeleznyov betegeskedett, aztán megszakította kapcsolatát az ügyvédjével. Maga vette kézbe az ügyét: a tárgyalást sikerült néhány hónappal elnapoltatnia.

Végül Szeleznyov mégiscsak beismerte bűnösségét és kézzel megírta bűnbánó levelét – benne a nehéz életútja történetével. Az ítéletét 2017 áprilisában hirdették ki, amikor az orosz hekkerek feltételezett beavatkozása az amerikai elnökválasztásba már néhány hónapja az amerikai média egyik legfőbb témája volt. Szeleznyovot huszonhét évre ítélték,[56] ami a leghosszabb idő, amelyet az Egyesült Államokban valaha is kiszabtak kiberbűnözésért. Ezt követően a hekker a bűnbánó retorikáját vádlóra változtatta. „Politikai fogoly vagyok. Fegyver az USA elnöksége számára – nyilatkozta Szeleznyov. – Jelezni akarnak az egész világ számára, engem használva játékszerként. Számításba véve a fejemet ért sérülést, a mai döntés halálos ítéletnek tekinthető." Apja a döntést „emberevő ítéletnek" nevezte.

2017 szeptemberében Roman Szeleznyov még két ügy kapcsán elismerte[57] az ellene felhozott vádakat: az ezek által okozott veszteségek körülbelül ötvenkétmillió dollárt tettek ki.

*12. fejezet*

## A startupper

A titkosszolgálatok nem csak azokra vadásznak világszerte, akik valamikor a CarderPlanet-fórumot látogatták. Az utóbbi években az USA világszerte nem kevesebb mint tíz orosz hekkert tartóztatott le. Vannak, akiket elítéltek, mások az ítéletre várnak. Az orosz hatóságok ezeket az lefüleléseket többnyire „emberrablásként" aposztrofálják – és a szóban forgó orosz férfiak letartóztatásának módja néha tényleg erre emlékeztet.

2009-re a huszonöt éves Nyikita Kuzmin sikereket ért el mind legális üzleti, mind alvilági hekkertevékenysége terén. Társalapítója lett a YouDo társaságnak és megírt egy cikket[58] a weboldalindításról a roem.ru-nak. Akkoriban a YouDo nem a hétköznapi szolgáltatásokra specializálódott, mint most, hanem reklámkampányok megrendelési felülete volt. Körülbelül ugyanekkor jutott Kuzmin tudomására, hogy informatikai biztonsággal foglalkozó szakemberek felfigyeltek az általa végrehajtott feltörésekre: vizsgálni kezdték azt a trójait,* amit Kuzmin az utóbbi években dolgozott ki, és amivel százezer dollárt keresett.

Kuzmin nem más, mint a zenész Vlagyimir Kuzmin fogadott fia. „Nyikitának van apja, én csak felneveltem őt – nyilatkozta[59] a muzsikus 2010-ben. – Üzletember lett. Lehet, hogy a vér szerinti apjára hasonlít, akit egyszer se látott az életben." 2016-ban a művész már tagadta[60] a hekkerrel való kapcsolatát: „Ez nem az én fiam, ez egy hiba."

„A kisfiam a szeretőmtől született – mesélte[61] a hekker

* Lásd *Fogalomtár.*



édesanyja, Tatyána Artyomova. – Most Amerikában él, egy igazi számítógépzseni, rendszeresen küld nekem pénzt. Emlékszem, amikor Vologya eljött hozzánk, hogy megismerkedjen Nyikita apjával, azzal a férfival, akinek nem fogom megmondani a nevét. Kuzmin kezet szorított vele, sikereket kívánt neki, én pedig átadtam Kuzminnak a bérelt lakás kulcsait."

A periratokban[62] Nyikita Kuzmin arra hivatkozott, hogy két műszaki főiskolán is tanult, ahol „haladó számítógépes készségekre" tett szert. Az interjúalanyom, aki jó ismerőse a hekkernek, azt mondta, Kuzmin a Bauman egyetem információbiztonsági szakán végzett.

Nyikita a 2000-es évek közepén kezdte feltörni az ICQ-t: „ellopta" a tulajdonosok felhasználói fiókjait, és pénzt követelt azok visszaszolgáltatásáért. Ezzel a hekker körülbelül húszezer dollárt keresett. Nagyjából ugyanekkor megszerezte a hozzáférést az egyik pénzügyi szervezet felhasználónév- és jelszóadatbázisához is. Éveken keresztül hordta ki a bankokból a pénzt a világ minden táján: összesen körülbelül ötvenezer dollárt. Kuzmin időközönként különböző hekkerszoftvereket vásárolt, hogy az USA és Ausztrália bankszámláiról pénzt lopjon, de a programok gyakran nem működtek, ezért elhatározta, hogy csinál magának egy sajátot.

Megbízott egy programozót, aki tíz hónapon keresztül írta Kuzmin tervei szerint a banki trójait, amely a Gozi nevet kapta. Ezért a munkáért Kuzmin körülbelül húszezer dollárt fizetett.

Hogy saját fejlesztését népszerűsítse, 76service álnéven kezdett működni. A program nem pusztán vírus volt, hanem a kódtörő képességek nélküli bűnözők számára készült B2B-szoftver. Kuzmin bérbe adta a programot más hekkereknek: körülbelül heti kétezer dollárért meg lehetett szerezni a hozzáférést a Gozihoz, és be lehetett állítani a szükséges célokra.

A program az áldozatoknak fertőzött PDF-dokumentumokat küldött. A fertőzést követően a a Gozi egy vírust

töltött fel a számítógépre, amely ellopott minden titkos banki adatot, többek között a felhasználói fiókokba való belépéshez szükséges felhasználóneveket és jelszavakat is. Az információk aztán átkerültek a *Gozi* tulajdonosához is, Kuzmin kliensei pedig mindehhez hozzáférhettek egy kényelmes felületen. Amikor a nyomozók később rábukkantak a szerverre, amin nagyjából tízezer banki accounthoz szükséges felhasználói nevet tárolt, ezek körülbelül háromszáz céghez és szervezethez tartoztak, beleértve a NASA-t is. A hekkerek összes támadásának az Egyesült Államokban negyvenezer számítógép volt kitéve. A hekkerek okozta kárt az amerikai hatóságok nagyjából ötvenmillió dollárra becsülik.

2010-ben az FBI ügynökei a Gozi értelmi szerzőit keresték. Eddigre már tanulmányozták a trójait, és tudták az IP-címeket is, amelyekről a támadások indultak. A titkosszolgálatok megkapták az engedélyt, hogy megszerezzék az ismeretlen orosz hekker levelezését. Ennek egy részét csatolták a periratokhoz.

„Miért kell neked Zeus [a világ legkeresettebb hekkerének, Jevgenyij Bogacsevnek a vírusa]? Használd az én trójaimat. Az enyém jóval gyorsabb" – írta a hekker.

„Mennyibe fogsz nekem kerülni?" – kérdezte az ismeretlen.

„Két kilóba havonta, mindennel együtt. Ráadásul van botnetem* és könnyen kezelhető adminpanelem.

Egyéb fórumposztjaiban a Gozi értelmi szerzője azzal dicsekedett, hogy nemrégiben a barátnőjét megajándékozta azzal, hogy készülhetett róla egy fotósorozat a *Playboy*-ban, Európát pedig körbeutazzák egy BMW 6-os cabrióval.

Elkobzott levelezéséből kiderült, hogy a hekker az ügyfelének meghagyta, hogy a programért az Alfa Banknál vezetett számlájára küldje a pénzt, Nyikita Kuzmin nevére. Segített a titkosszolgálatoknak a hekker azonosításában

* Lásd *Fogalomtár.*



a nikita@youdo.ru e-mail-címének levelezése is. Az amerikaiak Kuzmin felhasználói fiókját az Odnoklassznyikin* is vizsgálták, és ott olyan fotókat találtak, amelyeken a hekker a BMW 6-os mellett áll: nyilván ez ugyanaz az autó, amellyel beutazta Európát.

2010. november 19-én Kuzmin ezt írta az egyik chatben: „Elutazom Thaiföldről, és valahol el fogok tűnni." Három nap múlva közölte, hogy Bangkokban van. November 27-én San Franciscóban tűnt fel, ahová munkaügyben utazott, nem is gondolt arra, hogy letartóztathatják. A repülőtéren Kuzmint azonnal letartóztatták, és átszállították egy New York-i börtönbe.

Amikor erről tudomást szerzett a Gozival dolgozó többi hekker, bepánikoltak. A Kuzmin által kidolgozott program egyik felhasználója ezt írta: „Mindenkinek, akinek dolga van a 76-os paranccsal, tartson mértéket, változtasson nevet a fiókjaiban, a fórumokon legyen óvatos, s ha nincs rá különösebben szüksége, ne hagyja el az országot, különben vége van." Egy másik felhasználó ezt írta: „Nyikita sokat fecsegett magáról, állandóan a jabberen ült,** és adta fel a partnereit..."

Kuzmint az elején az fenyegette, hogy kilencvenhét éves koráig lesz a börtönben. A vádat Kuzmin ügyében New York déli kerületéből Preet Bharara képviselte. Rámutatott,[63] hogy Kuzmin, miután átengedte a trójait a szolgáltatást igénybe vevőnek, „azt minden olyan ember számára hozzáférhetővé tette, akik híján vannak a számítógépes ismereteknek. A legtöbb (kiber)bűnténytől eltérően Kuzmin bűntettét, azaz a vírus elterjesztését és használatát nem lehet megállítani azzal, hogy elfogjuk azt, aki létrehozta. Kuzmin eladta másoknak a Gozi kódját, ezért ezt tovább lehet használni" – magyarázta az ügyész.

* Jelentése: osztálytársak. – *A fordító megjegyzése.*

** Azaz gyakran használta a Jabber elnevezésű üzenetszolgáltatót. – *A szerző megjegyzése.*

2011 májusában Kuzmin aláírta az együttműködésről szóló megállapodást, és elkezdett harcostársai ellen vallani: ezután sorra tartóztattak le hekkereket Rigában és Bukarestben.

Kuzmint az az Alan Futerfas védte,[64] aki az amerikai elnök fia, az ifjabb Donald Trump ügyvédje is. Korábban Futerfas olyanokat védett, akik a maffiával álltak kapcsolatban, Trump fiával viszont azt követően kezdett együttműködni, hogy kiderült a találkozása Natalja Veszelnyickaja orosz ügyvéddel: állítólag ez a nő ajánlotta[65] a Trump elnökjelölti stábjához tartozó munkatársaknak, hogy kompromittálják Hillary Clintont. Kuzmin ügyét sokáig vizsgálták, a tárgyalásokat folyton elnapolták.

A börtönben a hekkernek láthatóan volt hozzáférése az internethez. 2011-ben el tudta adni a YouDo-ban lévő részesedését, 2015-ben frissítette a fotóit a Facebookon, az ítélete előtt két hónappal kommenteket hagyott a *Roem* weboldalon. Például 2016. március 7-én részt vett abban az elnöki adminisztráció által kezdeményezett megbeszélésen,[66] amely azt célozta, hogy bocsássák az adóhivatal rendelkezésére az oroszok összes külföldi vásárlásaival kapcsolatos információt. „Ez egyenesen szenzációs" – jegyezte meg Kuzmin.

A hekker ítéletét 2016. május 2-án hirdették ki.[67] Három év börtönt és hétmillió dollár pénzbüntetést szabtak ki rá – ekkorra már öt évet töltött le. Ugyanezen a napon Kuzmin visszatért Oroszországba. A vád kétszer annyi letöltendő büntetést kért, de a bíróság figyelembe vette Kuzmin együttműködését az eljárás során.

Facebook-profilja alapján[68] Kuzmin jelenleg egy internetes kereskedelmi felülettel foglalkozik, és sokat utazik: szabadulása óta járt már Bécsben, Amszterdamban, Kijevben, Abu-Dzabiban, Szocsiban, a Putorana-fennsíkon és Jakutföldön is. Mindemellett elhatározta, hogy vallást alapít, amely minden embert egyesít a földön. Azt viszont, hogy velem erről beszélgessen, visszautasította.

*13. fejezet*

## A sportember

2012. március 22-én az akkoriban legsikeresebb e-sportliga, a Moscow Five vezetője, Dmitrij „Szmelij"* Szmiljanec bejelentette,[69] hogy a csapatnak lesz egy „kurátora", mégpedig az üzletember és dollármilliárdos[70] Szergej Matvijenko személyében. Ő Valentyina Matvijenkónak, az orosz Szövetségi Tanács, vagyis a parlament felsőháza elnökének a fia. Mint Szmiljanec elmondta, a Matvijenkóval folytatott tárgyalások alatt a Moscow Five csapata a League of Legends világbajnokságon sorra nyerte a meccseket. A Moscow Five weboldalán megjelent egy közös fotó Szmiljanecről és Matvijenkóról: Szmiljanec egy sötétkék Adidas inget viselt, Matvijenko fia pedig mellette ült egy kitömött bivallyal.

A közösségi oldalak tanúsága szerint Szmiljanec általában vonzódott a politikához, és sokszor volt kapcsolatban orosz közéleti személyiségekkel. 2012 márciusában, amikor Oroszországban elnökválasztást tartottak, egy szavazócéduláról készült fotót tett közzé[71] a Vlagyimir Putyin neve mellé tett kis pipával. A fényképet alá is írta: „Benne bízunk! Az erős vezető mellett vagyunk!" Egy kis idő múlva az elnöki hivatal adminisztrációja képviselőinek kerekasztaláról posztolt egy fotót,[72] ahol az „Oroszország e-sportjával kapcsolatos kérdéseket tárgyaltunk meg". Egy másik fotón az orosz zászló szerepelt, amely fölé egy idé-

* A vezető nevében szereplő „szmelij" ragadványnév jelentése: bátor. – *A fordító megjegyzése.*

zetet helyeztek a himnuszból: „Erőt ad nekünk a hazához való hűség."

Szmiljanec minden egyes verseny előtt nyilvánosan fordult az Istenhez: „Uram, segíts, hogy győzelmet arathassunk az Intel Extreme Masters felett Hannoverben. Moszkva becsületéért, Oroszország anyácskáért küzdünk!" – írta 2012 márciusában. Ugyanekkor tett közzé egy képet[73] *Egy áldott reggel Moszkvában* címmel, amelyet elmondása szerint Nyikasz Szafronov festőművész adományozott a Moscow Five-nak. A művészről köztudott, hogy orosz politikusokról és híresség ekről fest portrékat.

A Bloomberg adatai szerint[74] Szmiljanec 2003-ban ismerkedett meg Vlagyimir Drinkmannal, mindketten Counter-Strike-ot játszottak. Szmiljanec cheat-kódokat használva gyakran csalt. Hamarosan találkoztak. Drinkman elmesélte, összebarátkoztak: Szmiljanec olyan ember volt, akivel el lehetett menni vodkát inni és horgászni.

Drinkman Sziktivkarban nőtt fel, az általános iskola óta rajongott a számítógépekért, önállóan tanulta meg a C++ programozói nyelvet, és rendszergazdaként dolgozott az egyetemen. Szmiljanec Moszkvában született, ahol a Bauman egyetem információbiztonsági szakán végzett. Önmagáról a Twitter-oldalán annyit írt, hogy érdekli a geopolitika, az e-sport és az információbiztonság.

Drinkman érintkezett valódi rablókkal is: az egyik hekkertagtól tudni, hogy Drinkman személyes ismerősei közé tartozott a fanatikus Mihail Krug, ám őt 2003-ban egy golyóval megsebesítették, amikor egy autóban ült az egyik „törvényes tolvajjal" – aki viszont a támadás következtében életét vesztette.

Az amerikai büntetőeljárás adatai szerint[75] a két barát 2005-től kezdett behatolni pénzügyi társaságok, fizetési rendszerek és webáruházak számítógépes hálózatába, megszerezve a hozzáférést a hitelkártyák adataihoz. Szmiljanec felelt ezek viszonteladásáért is: a kártyák egyenként tíz és ötven dollár közötti összeget hoztak, a kibocsátó országtól függően. Megszállták a Nasdaq tőzsdét, a 7-Eleven szupermarketet, a francia Carrefour ruházati bolthálózatot és más óriásvállalatokat. Az elkövetkező tíz évben a vád adatai szerint körülbelül százhatvanmillió hitelkártyát loptak el és háromszázmillió dollárnyi kárt okoztak. Az amerikai titkosszolgálatoknál Drinkmant Albert Gonzalez hekker dobta fel (velük állt kapcsolatban a belorusz hekker, Szergej Pavlovics is), és már Drinkmanon keresztül mentek rá Szmiljanecre. Maga Gonzalez már húszéves börtönbüntetését tölti, amit százharmincmillió dollár értékű hitelkártya ellopásáért kapott.

2013 júliusában a titkosszolgálatok rátaláltak Szmiljanec Instagramján egy fotóra, amelyen Amszterdam belvárosában egy Oroszország címerével díszített kapucnis felsőben pózol. Ezt követően az amerikaiak a közelben lévő összes hotelt körbetelefonálták: az egyikben azt mondták nekik, hogy Szmiljanec tényleg a szállodában lakik, de jelenleg alszik. Másnap reggel a nyomozók megjelentek szálloda recepciójánál. Kiderült, hogy Szmiljanec két szobát vett ki. A szomszédban az a Vlagyimir Drinkman volt, akinek a tartózkodási helyére a titkosszolgálatok mindaddig nem tudtak rájönni.

A letartóztatása előtt, az utolsó VKontakte-posztjában Szmiljanec közzétett egy e-sportolókat ábrázoló fotót, a következő felirattal: „Oroszország e-sportjának közkincsei. Róluk rosszat csak a CIA és az MI-6* ügynökei tudnak mondani." Letartóztatása után Szmiljanecet elkezdték az e-sport „keresztapjának" nevezni, és a sports.ru is[76] egy cikkben azt írta, „most már mindenki számára világos, honnan volt pénze Szmelijnek a csapatok finanszírozására". Később a vizsgálatot végzők közölték, hogy a csoportban volt még három hekker, két orosz és egy ukrán, de őket nem sikerült elfogni.

Szmiljanec apja, a moszkvai ügyvéd, Viktor Szmiljanec

* Az egyik brit titkosszolgálat, a hírszerzés rövidítése.

úgy véli,[77] a fia bűnösségét semmiféle bizonyíték nem támasztja alá. Szerinte az őrizetbe vételekor Szmiljanecnél nem volt ott a legfőbb potenciális bizonyíték, a számítógép. „Még nagyobb kétségeim vannak a bankok és más pénzintézetek anyagi kárának összege felől is, ezek hihetetlen számok – írta az idősebb Szmiljanec. – Az amerikaiak szeretnek csillagászati összegekkel dobálózni, ezáltal törölni a milliárddolláros adósságaikat."

Szmiljanec szinte azonnal beleegyezett kiadatásába az Egyesült Államok számára. A New Jersey-i börtönbe került, ahol az időt a spanyol és a kínai nyelv tanulásával ütötte el. Drinkman két és fél éven át harcolt a kiadatása ellen. Azt nyilatkozta[78] a Bloombergnek, hogy a holland börtönben elolvasta George R. R. Martin *A tűz és jég világa* című művét. Interjút a börtön pszichiátriai részlegéről adott: ügyvédje szerint ide a hekker azután került, hogy Hollandia beleegyezett Amerikába történő szállításába.

2015 szeptemberében Szmiljanec és Drinkman is beismerte bűnösségét. Az ítélethirdetést többször elnapolták. 2018 februárjában Drinkmanra tizenkét év börtönt szabtak ki. Szmiljanecre négy évet, amit már le is ült a vizsgálat időtartama alatt. A bírósági ülésteremből szabadon bocsátották.

*14. fejezet*

## Az ügyvéd

2009-ben egyik este, egy prágai lakásban, ahol a feleségével élt az Oroszországból menekült Dmitrij Naszkovec, elment az áram. Néhány perc múlva csengettek. Amikor a feleség kinézett a kukucskálón, egy Electrics feliratú narancssárga mellényes férfit látott. „Ó, Gyima, nyiss ajtót, én köntösben vagyok!" – kiabálta Naszkovecnek a felesége. Amikor a férfi kinyitotta az ajtót, a lépcsőházban a villanyszerelőn kívül ott álltak az FBI ügynökei és a cseh rendőrök. Naszkovec előtt felmutatták az amerikai letartóztatási parancsot, megbilincselték, és bevitték az őrsre.

Naszkovec volt az egyik legsikeresebb orosz nyelvű hitelkártyacsaló: ahogyan azt később elmesélte,[79] ebben a foglalkozásban még csak nem is a pénz vonzotta, hanem „egy különös, zárt klubhoz" tartozás (a barátnője viszont, amikor Naszkovec kezdett meggazdagodni, „Paris Hiltonná változott"). Őrizetbe vétele után a fehérorosz férfi megkönnyebbült. „Végre-valahára ez a furcsa időszak [a várakozás a letartóztatásra] véget ért – emlékezett vissza. – Amikor meglátod a parancsot, amely fehéren-feketén kimondja, hogy a következő negyven évet börtönben fogod tölteni... Maga a börtön nem félelmetes. Annál fájdalmasabb az irreális szám: ez már agyrém és valami szürreális dolog!"

Naszkovecet Arkagyij Bukh ügyvéd, egykori bakui menekült védte, aki a 1990-es évek elején emigrált az Egyesült Államokba. New Yorkba érkezve azonnal jogászként

kezdett dolgozni a bevándorlókkal kapcsolatos vízumok, támadások és zaklatások ügyeiben. 2013-ban azt az Azamat Tazsajakovot védte, aki a bostoni maratonon történt terrortámadást végrehajtó Carnajev fivérek ügyének volt az egyik érintettje. Az utóbbi években Bukh a kiberbűnözők védelmére szakosodott, például ő volt a védőügyvédje Vladiszlav Horohorinnak és néhány más olyan orosz hekkernek, akiket az USA-ban ítéltek el.

„Ő a csokornyakkedős, kalapos, fehér nadrágos Osztap Bender* – jellemezte Bukhot az egyik védence. – Az FBI tette híressé, mert nagy csinnadrattával csúsztatta alája a klienseket. Hiszen az FBI minden egyes alkalommal azt a benyomást akarja kelteni, hogy komoly bűnözőt tartóztatott le – az adófizető állampolgárok örömére és a hivatali előmenetel érdekében. Mindennap a történelem legjelentősebb letartóztatása történik."

Bukh szerint az orosz hekkereket „orosz katonáknak" lehetne nevezni. Az Egyesült Államokat támadják, és nincs ezzel semmiféle morális probléma. Oroszországban a hekkerek megállapodtak az FSZB ügynökeivel, és nem nyugtalankodnak, mert pontosan tudják, hogy nem ültetik le őket – magyarázta Bukh. – Sok idő megy el a kutatásokra, támadásokra és más effélékre. Teljesen biztosak a büntethetetlenségükben. A legrosszabb esetben pénzt fognak adni vagy pénzt fognak kapni a feltételes börtönbüntetésért."

Bukh egy ideje nemcsak jogi szolgáltatásokkal foglalkozik, hanem megalapította a kibervédelemre szakosodott CyberSec nevű céget. Üzleti partnere Dmitrij Naszkovec: bár őt negyven év börtön fenyegette, az ügyvéd tanácsára a hekker vádalkut kötött, és már 2015-ben szabadult.

* Osztap Bender az Ilf-Petrov orosz szerzőpáros regényeinek, a *Tizenkét szék*nek és *Az aranyborjú*nak a népszerű hőse. – *A fordító megjegyzése.*



A céggel jelenleg tíz ismert hekker dolgozik, sokan közülük körözés alatt állnak. Maga Naszkovec ezt ezzel magyarázza: „Hogy hogyan harcoljunk az orosz rablók ellen, azt senki se tudja, kivéve magukat az orosz rablókat."

Azok a hekkerek, akikre az amerikaiak vadásznak, alapjában véve tiszteletben tartják az orosz kiberbűnözők alapszabályát: „ne a .ru területén működj", ne lopj a saját országodban. Ha ezt mégis megkockáztatják, akkor néhányukat a saját államuk fog el.

*15. fejezet*

# A rejtőzködők

2015 nyarán az orosz Központi Bank létrehozta a FinCERT megfigyelőrendszert, amely a hitelfinanszírozási szféra számítógépes incidenseire reagál. Ezen a központon jelenthetik a bankok a számítógépes támadásokat, itt elemzik azokat, és védelmi ajánlatokat kapnak a titkosszolgálatoktól. Ilyen támadásból sok van: az orosz Sberbank 2016 júniusában kiberbűnügyek által okozott gazdasági veszteségét hatszázmilliárd rubelre becsülik.[80] Ekkor alapították a bank Bizon nevű leányvállalatát, amely a vállalat informatikai védelmével foglalkozik.

A FinCERT munkájának eredményeiről szóló első jelentésben[81] (2015 októberétől 2016 márciusáig) huszonegy célzott, a bankok infrastruktúrájával szembeni támadást említenek, ezek nyomán tizenkét büntetőeljárást kezdeményeztek. E támadások nagy része egyetlen csoport kezében volt, amely magát Lurknak nevezte annak a vírusnak a tiszteletére, amelyet ők fejlesztettek ki, és amelynek révén loptak el pénzt a kereskedelmi vállalatoktól és bankoktól. A csoport tagjait a rendőrség és a kibervédelem szakemberei 2011 óta keresték. Hosszú ideig sikertelenül: 2016-ra a csoport körülbelül hárommilliárd dollárt lopott el az orosz bankoktól, többet, mint bármely más hekker.

A Lurk vírus különbözött azoktól, amelyekkel a nyomozóknak korábban dolguk volt. Amikor a programot laboratóriumban tesztelték, az semmit nem csinált (ezért is nevezték el Lurknek, az angol „rejtőzködik" szóból). Később kiderült,[82] hogy a Lurk úgy épül fel, mint egy moduláris rendszer: a program fokozatosan tölt be további, különböző funkciójú blokkokat, ilyen például a billentyűzeten beírt karakterek, loginok és jelszavak, vagy a monitor videóstreamjének lemásolása.



A vírus terjesztése érdekében a csoport olyan weboldalakat tört fel, amelyeket a bankok munkatársai látogattak: a tömegmédia internetes felületeitől (például RIA Novosztyi és Gazeta.ru) a könyvelési fórumokig. A hekkerek a bannercsererendszer sebezhetőségét használták ki, és ezeken keresztül terjesztették a kártékony programot. Néhány felületre csak rövid időre küldték be a vírust: egy könyvelőknek szóló lap portálján a vírus egy munkanapon ebédidőben, mintegy két óra hosszára jelent meg, de ez alatt az idő alatt is talált néhány neki megfelelő áldozatot.

A hirdetésre kattintva a felhasználó exploitokkal teli oldalra érkezik, ami után a megtámadott számítógépre kezdi gyűjteni az információkat – a hekkereket legfőképpen a távbanki szolgáltatások programja érdekelte. A bankok pénzügyi megbízási csatolmányait a nekik szükségesekre cserélték, és a nem megerősített átutalásokat átirányították azon társaságok számlájára, amelyek kapcsolatban álltak a hekkercsoporttal. A Kaspersky Lab munkatársa, Szergej Golovanov szerint az ilyen esetekben a csoportok az úgynevezett egynapos cégeket* preferálják, amelyeknek mindegy, hogy mit utalnak és mit váltanak készpénzre: a megkapott összeget rögtön készpénzre váltják, táskákba pakolják szét, és „zálogokat" hagynak a városi parkokban, ahol azokat felmarkolhatják a hekkerek.

A csoport tagjai szorgalmasan takargatták a tevékenységeiket: rejtjelezték az összes szokásos levelezésüket, hamis felhasználóként regisztráltak felületekre. A támadók tripla VPN-kapcsolatot, Tor böngészőt és titkos chatet használnak, de még a hibakereső mechanizmus is kudarcot vallhat – magyarázza Golovanov. – Hol a VPN kapcsol szét,

* Az orosz szakzsargonban azon cégek, amelyeket adóelkerülés miatt hoznak létre, valódi tevékenység nélkül.

hol a titkos chat bizonyul nem is annyira titkosnak, hol pedig valaki ahelyett, hogy a Telegramon keresztül hívna fel valakit, egyszerűen a telefont használja. Ez az emberi tényező. És ha az évek során felépült az adatbázisod, akkor ebben meg kell találni a véletlenszerűségeket. A bűnüldöző szervek azután kapcsolatba lépnek az internetszolgáltatóval, hogy megtudják, kié volt az adott IP-cím. És akkor felderítik az egész ügyet."

A Lurk hekkereinek őrizetbe vétele[83] akciófilmbe illő volt. Az MCSSZ* munkatársai egy összehangolt támadásban szerte Jekatyerinburgban feltörték a hekkerek lakásaajtajainak zárjait, aztán nagy erőkkel betörtek és lefogták a hekkereket, a padlóra fektették őket, majd átkutatták a helyiségeket. A gyanúsítottakat ezután autóbuszba ültették és kivitték a reptérre, aztán felültették őket egy teherszállító repülőgépre, amely Moszkvába repült.

A hekkerek garázsaiban számos autót találtak – drága Audikat, Cadillaceket, Mercedeseket. Találtak egy órát is, amely 272 briliánssal volt kirakva. Elkoboztak[84] tizenkétmillió rubelnyi ékszert és fegyvert. A rendőrség összesen körülbelül nyolcvan házkutatást tartott tizenöt régióban, és hozzávetőlegesen ötven embert vett őrizetbe.

A letartóztatott emberek nagy része a csoport informatikai szakembere volt. A Kaspersky Lab munkatársa, Ruszlán Sztojanov, aki a titkosszolgálatokkal karöltve a Lurk által elkövetett bűntények feltárásával foglalkozott, azt mondta, sokukra a csoport vezetősége olyan hétköznapi honlapokon bukkant rá, amelyek távmunkára kerestek munkatársakat. Arról, hogy a munka illegális lesz, a hirdetésekben természetesen semmit nem közöltek, de a Lurk a piacinál jóval magasabb fizetést ajánlott, emellett pedig otthonról lehetett dolgozni. „A hétvégét kivéve minden reggel az Oroszország és Ukrajna különböző régióiból származó, egymástól független személyek leültek a számítógép elé, és nekiálltak dolgozni – írta Sztojanov. – A programozók finomították [a vírus] aktuális verziójának funkcióit, a tesztelők ellenőrizték, aztán a botnetért felelős munkatárs mindezt feltöltötte a vezérlőszerverre, s ezt követően frissült automatikusan a vírus a botnet számítógépein.

A csoport ügyének vizsgálata a bíróságon még 2017 őszén kezdődött, és egészen 2019 elejéig tartott – az ügyirat terjedelme miatt, amely körülbelül hatszáz kötetet tett ki. A hekkerek védője, aki nevének elhallgatását kérte, közölte,[85] hogy a gyanúsítottak közül senki nem fog vádalkut kötni, néhányan azonban a tetteik egy részét beismerték. „Ügyfeleink valóban dolgoztak a Lurk-vírus fejlesztésén, de sokuk nem volt tudatában annak, hogy ez egy trójai program – magyarázta az ügyvéd.[86] – Egyesek az algoritmusok egy részét készítették el, amelyeket sikeresen lehetett [legálisan] használni a keresőrendszerekben is." A csoport egyik hekkerének az ügyét külön eljárás alá vonták: ő öt évet kapott, s ebbe a büntetésbe beleszámították a jekatyerinburgi repülőtér hálózatának a feltörését is.

Oroszországban az utóbbi évtizedben a titkosszolgálatoknak sikerült megsemmisíteniük a legnagyobb hekkercsoportok nagy többségét, azokat, amelyek áthágták a „ne dolgozz a .ru területén" alapszabályát: a Carberpet (körülbelül másfél milliárd rubelt loptak az orosz bankok számláiról), az AnunAkot (több mint egymilliárd rubelt tulajdonítottak el az orosz bankok számláiról), a Paunchot (a támadások számára platformokat hoztak létre, amelyen keresztül az egész világ fertőzéseinek körülbelül a fele ment át) stb. E hekkercsoportok jövedelme a fegyverkereskedőkével mérhető, amiben benne van annak a tucatnyi embernek a jövedelme is, akik közvetlenül a hekkerek mellett dolgoztak, többek között az őrök, a sofőrök, a tőkét illegális úton készpénzre váltók, s azoknak a weboldalaknak a tulajdonosai, amelyeken az új exploitok megjelentek.

* Az orosz Rendkívüli Ügyek Minisztériumának rövidítése.

*16. fejezet*

## A nyomozók

A kiberbűntények feltárásával mások mellett az orosz Belügyminisztérium egyik speciális alosztálya foglalkozik – ezt nevezik „K" ügyosztálynak. A Lurkhöz hasonló csoportok miatt itt fejlesztettek ki egy különleges elemzőprogramot az olyan kapcsolatoknak a feltárására, amelyek felett esetleg elsiklottak a vizsgálatot végzők, ha már túl sok összegyűlt információval volt dolguk: felfedett IP-címek, szerverek adatai, illetve olyan hekkerekkel kapcsolatos információk, akiket korábban hasonló eljárásoknak vetettek alá.

A „K" ügyosztály rendőrei a moszkvai Petrovkán található, egy minden gyanú felett álló, az egykor a kereskedő Kirjakov tulajdonában álló házban működnek, a Nagy Péter-kolostorral szemben, és két percre egy melegbártól. Az épületbe (amely korábban műgyűjtők, Mihail Obolenszkij herceg, egy orvos és egy fogorvosi iskola tulajdonát képezte) a 1990-es évek végén költöztek be, amikor elfogadták azt a határozatot, hogy létrehoznak egy, a Belügyminisztérium alá tartozó speciális, a kiberbűntények ellen harcoló alosztályt. „Akkoriban jelentek meg a kártyások, és már akkor világos volt, hogy az egyik alapvető irányvonalunkká a gyermekpornográfia terjedése elleni fellépés lesz" – mesélte a *Meduzá*nak Alekszandr Vuraszko, a hivatal igazgatóhelyettese.

Az intézmény munkatársai ritkán járnak dolgozni rendőr egyenruhában: többnyire farmer van rajtuk, az ingük kilóg, egyik-másik karján pedig ott az Apple Watch. A látogatóknak a bejáratnál kézzel állítanak ki belépési engedélyt; az első emelet folyosóján ajándékokkal teli vitrin. Darabjai között látható egy hagyományos orosz népi festéssel készített porcelánváza, a Külső Felderítési Szolgálat ajándéka, mellette pedig kézműves termék: felfűzött bagelkarikák.



A házban a legbonyolultabb kiberbűntényekkel foglalkoznak: azoknak a hekkereknek az ügyeiben nyomoznak, akik csoportokba szerveződnek, és kiválóan tudnak rejtőzködni. A hivatalban néhány tucat munkatárs dolgozik, az ügyosztályba kerüléshez az „operatív, a jogi és az informatikai" képességeket egyszerre követelik meg tőlük. Ilyen embereket nehéz találni, vannak, akik a belügy moszkvai egyetemről vagy a Bauman Állami Egyetemről érkeznek, de feltétlenül szükséges a továbbképzésük.

A rendőrök a saját ügyosztályaikon reggelente egy gyors értekezletre összegyűlnek, s péntekenként a vezetés minden hivatali dolgozót összehív. Egyes kollégák reggel öt óra körül kezdenek: ebben az időben kell kiszállniuk az őrizetbe vételekhez. Amelyeken egyébként nincs mindenki jelen: egy steril szobában, ahol nincs internetelérés, vizsgálják az elkobozott adathordozókat és más technikákat.

„Ezt 1999-ben általános programozási ügyosztálynak lehetett volna nevezni – meséli Vuraszko. – De mára mindenki rendkívül szűk területekre specializálódott. Előfordul, hogy nem vagyunk képesek kiigazodni, és olyankor nincs értelme státuszban tartani olyan szakembereket, akik visszafejtik a kártékony programokat, amikor olyanokhoz is lehet fordulni, akik ezzel keresik a kenyerüket, mint amilyenek például a Group-IB, a Kaspersky Lab, a Positive Technologies alkalmazottai. Ezek aktív piártevékenységet tudnak folytatni [a nyomozásokkor], de csak mi, illetve az FSZB tehetünk pontot az ügyekre – vonzódunk a felelősséghez."

„A mi hősies rendőrségünk akkoriban nem értett a számítógépekhez – emlékezett vissza a 2000-es évek elejére az egyik hekker. – Az „R" ügyosztály [a jövőbeni „K" ügyosz-

tály] fél év múlva állt el egy banális lehallgatástól – pénzért. A nagy halat soha nem fogták el, és nem is fogják, mivel a nagy halnak Oroszországban akkoriban nem volt mit tennie. Az USA és Európa bankrendszere ötven évvel idősebb a miénknél, a mozgástér ott természetesen sokkal nagyobb. A leggyakrabban az emberek véletlenül kerülnek olyan helyzetekbe, amelyeknek semmi közük nincs a hitelkártyacsaláshoz."

Vuraszko szerint sokan az orosz rendőrök közül az alapvető számítógépes védelemmel sincsenek tisztában: nem tudják, mi az az IP, nem értik, hová kell kérdéseket intézni, hogy információkhoz jussanak az operatív-felderítő tevékenység során. A „K" ügyosztály gyakran tart a nyomozók és a bírák számára kurzusokat, hogy megértsék, miről is van szó kiberbűntettekkel kapcsolatos ügyek esetén.

A „K" ügyosztály az utóbbi években felderített néhány, a Lurkhöz hasonló ügyet. Az ezekkel kapcsolatos munka sokáig tart: a rendőrök mindig igyekeznek leleplezni a csoport összes tagját, és mint bűnszervezet ellen megindítani az eljárást – egyébként a gyakorlat azt mutatja, a hekkereket csak feltételes szabadságvesztésre ítélik.

– A csoport tagjai az egymás közötti érintkezésre általában a jabber és egyéb ingyenes messenger szolgáltatásokat használják. A szervezők minden kulcsmomentumot a védett csatornákon keresztül tárgyalnak meg – mondta Vuraszko a Lurk tevékenységének részleteiről.

– Azaz, ezekhez önöknek végeredményben nincs is hozzáférésük?

Válaszképp az őrnagy elneveti magát, és ezt mondja: „Engedje meg, hogy ne válaszoljak erre a kérdésre."

A „K" ügyosztályhoz tartozó rendőrök csak válogatott kiberbűntények ügyében nyomoznak. Soha nem vizsgálódnak az orosz ellenzékiek és a nem állami média elleni hekkertámadások ügyében, még akkor sem, ha bizonyítékokkal rendelkeznek: rendkívül bonyolult hozzájuk fordulni egy elektronikus postafiók feltörése vagy egy



vállalkozást érintő DDoS-támadás bejelentésével. Az ilyen bejelentéseket, több mint valószínű, hogy nem is fogadják.

„Az az igazság, hogy a virtuális térben a bizonyítékok összegyűjtése jóval bonyolultabb, mint a fizikaiban – magyarázta[87] Alekszej Lukackij, a Cisco Systems informatikai védelmének konzulense. – Az információkat apránként gyűjtjük be, és ez igen komoly erőforrásokat igényel. Belföldön elkövetett számítógépes bűntények – például egy hekkercsoport banki behatolása – nagyon gyengén deríthetők fel. Sem a törvényhozás, sem a nyomozók túlnyomó részének a képesítése nem teszi lehetővé a hatékony nyomozás lefolytatását. Minden egyes eljárás rendkívül bürokratikus, ezért mire kiadják a parancsot a videókamerákon fellelhető bizonyítékok összegyűjtésére, a nyomokat addigra már törlik." Lukackij szerint akkor tud működni az ilyen ügyek utáni nyomozás, „ha a károsultak között van olyan cég, amely a bűnüldöző szervek helyett össze tudja gyűjteni és fel tudja mutatni a bizonyítékokat" – ám ilyen esetben is a bíróság többnyire csupán feltételes letöltendőt szab ki a bűnelkövetőkre, akik azután ugyanúgy folytatják a ténykedésüket, mint korábban. Az ügyeket leginkább „az Oroszországi Föderáció büntető törvénykönyve 272., azaz a »Jogtalan hozzáférés számítógépes információhoz« cikkelye alapján tárgyalják."

A Lurkhöz hasonló nagy hekkercsoportok természetesen nem korlátozzák a tevékenységüket a jelenkori orosz internetes bűnözésre. Van egy másik hatalmas szegmens is – jelen vannak a darkneten, az internetnek azon a részén, amely el van zárva avatatlan szemek elől. Ennek a rétegnek szintén megvannak a főszereplői, és ahogy egykor a CarderPlanet esetén, ők is csupán a fórumok alapítóinak és adminisztrátorainak tűnnek.

*17. fejezet*

## Feketepiac

Az autó az erdő melletti út szélén állt meg, nem messze a moszkvai körgyűrűtől. Egy férfi szállt ki belőle, a kezében egy csomaggal. Körülnézett, odament az előírt útjelzőhöz, letette a földre a pisztolyt és a lövedékeket tartalmazó csomagot, és faleveleket szórt rá. Néhány óra múlva a vásárló az általa is ismert tájékozódási pontról elvitte a „zálogot".

A „zálogos" számára ez már megszokott rituálé volt: az utóbbi években kettős életet élt. A család, a barátok, a munkahelyi kollégák úgy tudták, imád a dácsáján pihenni. Soha nem mesélt nekik semmit arról, hogy néhány éve Moszkva központjában bérel egy hangszigetelt műhelyt, ahol lőfegyvereket gyűjt, hogy azokat alvilági fórumokon értékesítse.

Az orosz nyelvű darknetbe nagyjából öt éve került be. Minden érdekelte, amit nem lehet megtalálni a szokásos interneten: bélyegzők, útlevelek, kábítószerek, fegyvergyártás. Korabas nicknéven regisztrált a Runionra, amely Oroszországban az egyik legnagyobb darknetfórum. A fórumra a Toron keresztül lehetett bejutni, ezzel a titkosított böngészőprogrammal, amellyel a felhasználók úgy rejtőzködtek, akár a Harry Potter-es láthatatlanná tévő palást alatt, és beléphetnek olyan weboldalakra, amelyeket az átlagos keresők nem szoktak találatként megjeleníteni. A technológiát, amellyel a Tor dolgozott, az 1990-es évek közepén az amerikai flotta laboratóriumában hozták létre az amerikai állami intézmények hálózati védelmére. A későbbiekben feloldották titkos jellegét, és független fejlesztőknek adták



át. Jelenleg a program az egyik leghatékonyabb módja az internetes cenzúra megkerülésének és az anonimitás megőrzésének. 2013-ban Edward Snowden is a Toron keresztül juttatta el az amerikai Nemzeti Védelmi Ügynökség (NSA) dokumentumai egy részét az újságíróknak.

A fórumokat tanulmányozva Korabas összegyűjtötte a pisztolyokról fellelhető utasításokat. A gyártásra, ahogy arra számított is, sok pénz ment el, de amikor eladásra bocsátotta a fegyvert, váratlanul gyorsan megvették. Korabas ekkor elhatározta: nem áll meg, hanem próbál még többet hozzátenni a pénzéhez.

A felhasználó anonim módon bérelte a műhelyt, amelybe vett néhány munkapadot és fúrót. A helyiség fűtetlen volt, ezért kényelmesen csak tavasszal és nyáron lehetett benne dolgozni, de ha voltak rendelések, muszáj volt a hidegben is ott lenni. Történetének mesélése során Korabas gyakran használta az „emping" szóösszevonást, a „hogyha nem csal az emlékezetem" orosz szavak kezdőbetűiből létrehozott szót, az érintkezésünk pedig a titkosított chaten keresztül történt: megmutatni az arcát vagy megmondani a valódi nevét egyáltalán nem akarta. Néhány napig egyfolytában beszélgettünk, olykor a chatre új tagok is csatlakoztak, akik jó pár, a darkneten végrehajtott művelet részleteiről számoltak be.

A biznisz gyorsan fejlődött: Korabas hamarosan rátalált arra, aki a töltényeket értékesíti, és elkezdett hangtompítót gyártani. Ekkorra ő lett a Runionon az egyik legfőbb fegyverkereskedő. Amíg mások a viszonteladással foglalkoztak, Korabas jellel ellátott fegyvereket vásárolt, és azokat 9×18 milliméteressé alakította, amely az egyik legelterjedtebb kaliber volt a FÁK országaiban. Az átalakítás után Korabas minden egyes pisztolyt ellát hangtompítóval is, és a belvárosi műhelyében lövöldözik velük: „Lusta vagyok minden pisztolyt az erdőbe cipelni, hogy kipróbáljam. A moziban a hangtompítós pisztolyok hangtalanul lőnek,

a valóságban azonban még a legjobb esetben is 50 százalékos [a zaj]" – meséli.

A Toron történő fegyvereladás hobbi a számára: a „boltokban" az árak hatvanezer rubelnél kezdődnek, egy-két üzlet jön létre havonta, úgyhogy az éves nyereség körülbelül ötszázezer rubel. „Valóban nem lakásra kerestem" – írja Korabas, és kitesz három zárójelet: nevet. Egyébként a kedvenc időtöltése, hogy időközönként ő maga is kimegy a város határán túlra lőni. „A lövöldözésre nem a családi büdzsétől veszem el a pénzt, csak azt költöm rá, amit a Toron kerestem meg."

Korabas tisztában van vele, hogy bármelyik pillanatban őrizetbe vehetik, aztán ülhet jó pár évet, ezért nagyon óvatos. A számítógépén Linux operációs rendszer működik, a merevlemezei kódolva vannak, a hálózatra a Toron keresztül kapcsolódik, a keresetét pedig bankkártyákról veszi fel külföldön – ezeket a kártyákat olyan emberek nevére állították ki, akiket maga Korabas sem ismer.

Az orosz nyelvű darkneten ezrek élnek hasonló módon. Csak a Runionon naponta két-háromezer ember fordul meg. A Tor árusai és adminisztrátorai, akik többnyire a büntető törvénykönyv hatálya alá tartozó tevékenységekkel foglalkoznak, meglehetősen ritkán érintkeznek újságírókkal: úgy vélik, bármely óvatlan kontakt a letartóztatásukhoz vezethet.

* * *

A Runionhoz hasonló fórumokon nem pusztán fegyvereket lehet vásárolni, hanem feltöréseket is lehet rendelni, és hamis személyiséget is kreálhatunk magunknak. Makszim épp az ilyen fórumokon keres megrendelőket, és a leggyakrabban „kezesen", azaz egy speciális közvetítőn keresztül dolgozik, aki befagyasztja a kifizetést, amíg a rendelés nem teljesül, és dönt a vitás kérdésekben, amennyiben ilyenek felmerülnek. Makszim alapvetően phishinggel*

* Lásd *Fogalomtár.*



foglalkozik. A feltörés néha egy hónapot is igénybe vesz: az idő nagy része arra megy el, hogy lehetőleg minél több személyes információt gyűjtsön az áldozatról. Makszim az orosz ellenzékieket töri fel, és biztos benne, hogy nem egyszer dolgozott már a titkosszolgálatoknak is, bár azoknak az emberei soha nem beszélnek arról, hogy oda tartoznak.

Makszim azóta dolgozik a darkneten, hogy egy ismerőse majdnem börtönbe került feltörésért. Ugyanezt az utat járta be a mostani elfoglaltságáig egy másik hekker is, aki Sleepwalkernek nevezi magát. Amikor a barátja majdnem megégette magát, mert nem törődött az anonimitással, Sleepwalker megalkotta a saját számítógépes „profilját" (azaz „identitását"), és ezzel egy időben árulni is kezdte azt. Emellett az orosz nyelvű Toron őt úgy ismerik, mint azt a hekkert, aki bitcoinért teszteli a weboldalakat, hogy vajon lehetséges-e a feltörésük, valamint konzultációkat tart az anonimitásról.

Sleepwalker gyerekkorától nézte a hekkerekről szóló filmeket. „Ott ül valaki, feltör valamit, a képernyőn fekete a háttér, zöld betűk villognak, ez titokzatosnak tűnt" – emlékszik vissza. A Runionra írt egy cikket *Hekkernek lenni?!* címmel, amelyben a következő elvet vallotta: „A hekkerek örülnek, ha megoldanak egy problémát, megtalálják a kerülő utakat, megértik a folyamat lényegét." Ugyanitt Sleepwalker az arra igényt tartókat „a gyanús személy számítógépéről a bizonyítékok összegyűjtésére" és „a VKontakte oldalaira való betörésre" tanította. Egyébként nekem azt mondta, nem foglalkozik a közösségi oldalak és fiókjaink feltörésével – pénzért. 2014-ben Sleepwalker demonstratíve még el is lopta egy iskolás sráctól a Vkontakte felhasználói fiókját, illetve postafiókját, aki azt kérdezte, mennyibe kerül majd a feltörésszolgáltatás.

Néhány évvel ezelőtt Sleepwalker hozzáférést szerzett egyes útlevelek szkennelt képeihez és más iratok adatbázisához. Véletlenül történt, amikor jelszavakat válogatott az egyik webáruház szerveréről. Ezt követően a hekker

elkezdte „speciális módon kihúzni" a különböző társaságoktól a szkennelt dokumentumokat, és ezek mellé „személyiséget" is gyártott az interneten.

A munkát minden „személyiség" esetében azzal kezdi, hogy kigondol egy emberi történetet. Ezután „élni" kezd vele. A „kulcsrakész személyiségek" (= kitalált, felépített) számára regisztrál néhány accountot a közösségi hálón, fotókkal és két-háromszáz baráttal, ezeket kiegészíti „kitalált érdeklődési körökkel és apró részletekkel", az oldalakra a „személyiséghez" illő témákban posztokat ír, lemodellezi annak nyelvét, e-pénztárcát regisztrál a Yandexen és Qiwin, regisztrálja ezekre a „személyiség" telefonszámát, és olykor előfordul, hogy hozzáférést szerez internetfórumokhoz, hogy otthagyhassa a a „személyiség" kommentjeit.

Egy „személyiséggel" való munka körülbelül egy hónapot vesz igénybe. Néhány év alatt Sleepwalker körülbelül száz „személyiséget" adott el, s mindegyikért ötven-száz dollárt kapott.

„A létrehozáshoz elég figyelembe venni azokat az alapvető tényezőket, amelyek alapján a hálózatokon fent lévő emberek úgy vélik, hogy a személyiség igazi, akkor azzá válhatsz, akivé csak akarsz az internetszolgáltató, akár az átlagember vagy a bűnüldöző szervek számára – mondja a hekker. – Ennek hasznát lehet venni például zsaroláshoz, ami nemcsak azt teszi lehetővé, hogy egy bizonyos személy benyomását keltsük, hanem azt is, hogy valóban jelen lehessünk általa a virtuális térben. Például fogadjon és küldjön pénzt. És virtuális személyként érintkezzen."

Sleepwalker arról beszél, hogy ebben a munkában a legbonyolultabb a megalkotott „személyiség" ismereteit birtokolni, azaz helyesen írni és értelmes kommenteket hagyni. „Néha az account élettelibbnek bizonyul a hálózat hétköznapi használóinak accountjainál – mondja. – Egyszer felkértek, hogy hozzak létre egy okos és szép lányt, a külföldiek Facebookra vonzása és eszkortszolgáltatás



értékesítése érdekében. Folyót lehetett velük aztán rekeszteni."

Sleepwalker megalkotott egy egyetemi hallgatót, aki kalandokat keres, egy lányét, aki a darknet és a copywriting iránt érdeklődik. A maga számára pedig az öreg horgászét. Ezzel a személyiséggel szedte össze az útlevelek másolatait, e-pénztárcát hozott létre a Yandexen, a Qiwin, és profilt az Avito nevű online piacon. A VKontaktén lévő oldalát nem töltötte fel teljesen: „Öreg vagyok, legyen elég ennyi."

A hétköznapi interneten Sleepwalker kényelmetlenül érzi magát: „Az az érzésem támad, hogy valaminek vagy valakinek az ellenőrzése alatt állok."

* * *

2016. június 18-án megkeresett a darknet legnagyobb orosz nyelvű fóruma, a Runion képviselője. Felajánlotta, hogy interjút készít az orosz nyelvterületű darknet egyik leginkább tisztelt és legbefolyásosabb emberével. Ő volt Nikkon – a fórum adminoldaláról az az ember, aki kezességet is vállal az ügyletekért. Az üzletkötéseket azért követi nyomon, hogy azt és aszerint adjanak el, amiben megállapodtak. Ekkoriban kezdte az állami duma tárgyalni a Jarovaja-csomagot, az úgynevezett terrorizmus elleni törvénymódosításokat, amelyek csapást mérnek többek között az internet privát szférájára. A beszélgetési szándékot a Runion képviselője többek között a nyilvánosságra hozatali szándékkal magyarázta: „A Tor biztonságos a kommunikációhoz, és ott nem annyira pedofilok és kábítószerárusok gyűlnek össze, mint inkább azok, akik nagyra értékelik bármely információ szabad terjesztését."

Két évvel korábban, 2014 őszén, egy este Nikkon egy szállodai szobában ült Moszkvában; borozgatott és olvasgatta a saját fórumát. Korábban végzett a munkájával, mint tervezte, és másnap indult a repülőgépe. Kiküldetése ideje alatt végig törte a fejét, mit vehetne ajándékba a barátnőjének: „olyat akartam, ami nem banális".

Egyik ismerőse a Runionból váratlan ajánlattal fordult hozzá: segítsen eladni néhány tétel smaragdot.

Mint a fórum hivatalos kezese, Nikkon időnként kábítószer- és fegyvereladási ügyleteket is lefolytatott; kipróbálta az árut és százalékot kapott érte, ezzel akár három és fél millió dollárt is keresve havonta. Mindemellett az, hogy a Runionnál adminisztrátorként dolgozott, teljesen mindegy volt. „Az ügyleteimből származó jövedelmem és az alapfizetésem összemérhetetlen – mondja. – Számításba véve a piac növekedésének ütemét, lehet, hogy néhány év múlva [a helyzet] megváltozik."

Nikkon azt válaszolta, hogy benne van az ügyletben. A feladata az volt, hogy vegye fel a pénzt a vásárlótól, igazolja az összeg meglétét, és várja az eladótól az áru átadására vonatkozó jelet. A smaragdok minőségét másvalaki ellenőrizte.

Amikor végzett az ügylettel, elhatározta, hogy ékszert vásárol a barátnőjének. Nikkon először búját kliensi bőrbe. Mint bárki, aki „zálogot" vesz fel, izgult, hogy véletlenül se szaladjon járőrbe: törvénytelen ékszerkereskedésért öt év börtönt lehet kapni. Ezután a vásárlás után nem szándékozott a továbbiakban vásárolni a darkneten.

Nikkon ekkor már körülbelül egy éve volt a Runionnál. Innen átment a kártyások fórumaira – azokra, amelyek a CarderPlanet bezárása után jelentek meg.

Nikkon állítja, hogy ő maga nem foglalkozott hitelkártyacsalással, „csak olvasott és érdeklődött". A Torra „a tudásszomj vezérelte, hogy olyan ismeretekre tegyen szert, amelyek nyílt forrásokból elérhetetlenek". Mint mondja, a Tor ekkoriban „a ma is létező előítéletek gyűjteményét jelentette: mint amilyen a gyermekpornós oldalak, vagy azok a félelmetes és rejtélyes helyek, ahol akár az online játékok labirintusaiban, gyereksírás hangjai kísértenek. Az ilyen weboldalak miatt az alvilági internet hamar bekerült az orosz nyelvű netsztalkerek (azaz az interneten



azt extrém helyzetek iránt vonzódó, épp ezért elhagyatott helyekre behatolók) kamaszos mitológiájába, mint olyan hely, ahol »különleges feltételek« mellett lehet megtalálni az igazságot. A YouTube-on lehet a »mélyinternet« ez utóbbi jellegzetességéről ilyen videókat találni:[88] »egy csendes otthonról«, ahol állítólag letétbe helyeztek[89] információkat az Istenről, a halálról, az életről és mindenről, amit csak akartok."

A titkos, földalatti hálózatot tanulmányozva Nikkon beleütközött egy angol nyelvű fórumba, ahol kódolásról és kábítószerekről folyt az eszmecsere. Ezeket ő úgy fogta fel, mint aranybányát – a „nem klasszikus" tematika miatt. Azután más fórumokra is rálelt, egyébként ezek közül elég sok hamar megszűnt. Nikkon emlékszik például a Freedom Hosting bukására: tíz Tor-weboldalt is tároló tulajdonosát 2013-ban letartóztatták, és „a gyermekpornográfia világméretű terjesztése legfőbb közvetítőjének nevezték".[90] Interjúalanyom a projekt bezárását „a Tor elleni első komolyabb csapásnak" nevezte. Az FBI közölte,[91] hogy a szervereket már a tulajdonos letartóztatása előtt is megfigyelték.

A Freedom Hosting sebezhetősége a Tor sok orosz nyelvű részlegén keltett pánikot – a valódi kár amúgy csupán néhány weboldal bedőlésére korlátozódott. Az alapvető felületek – a Runion, a RAMP, az R2D2 és az Amberoad – folytatták működésüket. Az alapítók angol nyelvű kollégáiknál tájékozódtak, elsősorban a Silk Road weboldalon, amelynek ekkorra már valóságos kultusza alakult ki.

* * *

2010 végén a fiatal amerikai libertariánus, a könyvesboltban dolgozó Ross Ulbricht a naplójába a következő új ötletét jegyezte fel: „Létrehozni azt a weboldalt, ahol az emberek anonim módon azt vásárolhatnak, amit csak akarnak, és teljesen nyomtalanul." Néhány hónap múlva előállt a Silk Roaddal, ezzel az egész világra kiterjedő pénzpiaccal:

az első eladott árucikkekké a maga Ulbricht által termesztett varázsgombák váltak. Hamarosan ez más kereskedőket is idevonzott. A Silk Road először egyesítette a Tort a bitcoinnal, és használata elég egyszerű volt: az árucikkeket igen gyakran postán, DVD-tokokban küldték szét. A Silk Roadnak köszönhetően értesültek a Torról és a hálózati anonimitásról is a hétköznapi internetfelhasználók ezrei.

A titkosszolgálatok is tudomást szereztek a Silk Roadról: 2012 januárjában egy különleges csoportot hoztak létre a weboldal létrehozóinak felkutatására. Eddig maga Ulbricht, aki a Silk Roadon Dread Pirate Roberts néven szerepelt, már havi huszonötezer dollárt keresett jutalék formájában a portálon történő eladások után. A felületet nemcsak pénzkeresetre használta, hanem arra is, hogy publikálja a libertariánus prédikációit: „A gazdaság új típusát hoztam létre, hogy az emberek megérezzék, mi is az: a hatalom befolyása nélkül élni a világon." Meg volt róla győződve, hogy a felületén létrejövő minden egyes ügylet *újabb lépés az általános szabadsághoz.*

Az amerikai titkosszolgálatok végül leleplezték Ulbrichtot és a San Franciscó-i könyvtárban őrizetbe vették. 2015 májusában életfogytiglani börtönbüntetést szabtak ki rá. Az ítélet kihirdetése előtt Ulbricht levelet írt a bíróságnak: „A Silk Road lényege, hogy az embereknek szabadságot kell *adni önálló döntéseik meghozatalában. [...] A kielégülés* megfelelő eszközei felé kell terelni az ember kábítószerek iránti szenvedélyét. Rájöttem, hogy miközben szabadságot adsz az embereknek, sohasem tudhatod, mihez kezdenek vele."

Elveivel Ulbricht sokakat ösztönzött a 2012-es orosz alvilági kibermanifesztum létrehozására, amelyet ettől kezdve gyakran használtak a darknet fórumain: „Az internet veszélyessé vált az ember számára, el akarják tőlünk venni azt a jogot, hogy információkat cseréljünk, az internet ellenőrzötté válik, a szólásszabadságot korlátozzák, az embereket, akik a saját gondolataikat terjesztik, üldözik, s kamerákkal akarják minden lépésüket ellenőrizni." Emellett a kiáltvány szerzői rámutattak, hogy ők azok, akik „az igazságra ki vannak hegyezve". A fegyverek árusítását a fórumon azzal magyarázzák, hogy „mi magunk akarjuk eldönteni, hogyan és mivel védjük magunkat és a közeli hozzátartozóinkat", a kábítószerek árusítását pedig azzal, hogy „mi magunk akarjuk ellenőrizni, mi kerül a szervezetünkbe".

*18. fejezet*

## Oroszország fő spammerje

2013. április 1-jén az Antichat nevű portálra felkerült az egyik legismertebb orosz hekker posztja, aki Szevera álnéven működött.

*Pjotr Szevera vagyok, sokan ismernek az e-mailes hírlevélszolgáltatásom[92] révén, amelyet már tizenöt éve nyújtok. De minden mozgásban van, minden változik, és eljött az idő, hogy én is változtassak a munkám irányvonalán. Néhány nappal ezelőtt kaptam egy ajánlatot az orosz Szövetségi Biztonsági Szolgálattól (FSZB), hogy vezessem a Különálló Speciális Információbiztonsági Zászlóaljat (OSZBIB).*

*Ez egy új alosztály, amelyet azért hoztak létre, hogy ellenállást tanúsítson az USA, Kína, Németország és más országok kiberháborúival szemben. Az OSZBIB feladatai közé fog tartozni az Oroszországi Föderáció legfontosabb infrastrukturális objektumait fenyegető informatikai és elektronikus támadások operatív elhárítása, vagyis a fellépő fenyegetésekkel szembeni adekvát és operatív választevékenység.*

*Engem nemcsak a vezetéssel bíztak meg, hanem azzal is, hogy hozzam létre az OSZBIB legfőbb testületét. Természetesen az általam jelölt személyekre vonatkozó összes ajánlatot meg fogja tárgyalni a „K" ügyosztály és az FSZB Információbiztonsági Központja hivatalának vezetősége, de értésemre adták, hogy szinte teljes a cselekvési szabadságom a törzstestületre vonatkozóan. Az OSZBIB, teljes létszámát elérve, egy év múlva ötszáz fős alakulattá bővül, addig az is a megbízatásaim közé tartozik, hogy az első száz főt összetoborozzam. Nekünk nem fontos, hogy eddig mivel foglalkoztatok, a lényeg az, hogy meglegyen a munkához szükséges tudásotok és ismeretetek, va-*



*lamint az, hogy meg akarjátok védeni a Hazátokat és a közeli hozzátartozóitokat a 21. század reális fenyegetéseitől.*

*A jelentkezéshez szükséges:*

*– orosz állampolgárság,*

*– 18 és 45 év közötti életkor,*

*– az információbiztonság területére és ennek határterületeire vonatkozó mély és sokoldalú tudás,*

*– a nem szokványos megoldások gyors megtalálásának képessége,*

*– képesség a csapatmunkára,*

*– felsőfokú műszaki végzettség előnyt jelent, de nem kötelező, mert jóval fontosabb az, amit valóban tudtok. A hadtudományi tanszéken szerzett végzettség vagy az Oroszországi Föderáció haderejénél teljesített katonai szolgálat letöltése szintén előny.*

*A próbaidő után az általam kiválasztottak mindegyike megkapja az orosz szövetségi védelmi szolgálat, azaz az FSZB tisztjeinek járó összes juttatást, a továbbiakban pedig a tényleges tiszti rendfokozatokat. A munkahely Moszkva, a Szkolkovo, ahol most épül az OSZBIB munkatársai számára egy különálló tiszti épület. A ti és a családjaitok számára biztosított szállás a munkáltató számláját terheli, s egy különálló épületben, egy minden kényelemmel ellátott, 3p-s* telepen lesz. A fizetés 150 ezer rubel vagy még magasabb.*

*Már elkezdtem összeállítani a listát az első beszélgetéshez, küldjetek rezümét a jabber@honese.com-ra. Ha részt vettetek valami illegális dolog kidolgozásában, botnet, weboldalfeltörés stb., csatoljatok a rezüméhez egy rövid magyarázatot, de aztán ez már nem az én dolgom – bár az összes pályázónak teljes amnesztiát ígérnek, és garantálják, hogy nem fognak eljárást indítani azok ellen, akiket én nem választok ki, vagy nem tu-*

* A 3p Oroszország nagyvárosaiban a jelenlegi legkorszerűbb építészeti stílus, a legtöbb újonnan felhúzott lakóépület ezzel a modern, minden igényt kielégítő technikával épül. – *A fordító megjegyzése.*

*dok kiválasztani, de jobb bebiztosítani magunkat, és a hivatalos rezümében csak törvényes információt közölni.*

*A hazánk nevelt fel minket, megadott számunkra minden képesítést, így most eljött az idő, hogy mi szolgáljuk Oroszországot.*

A fórum résztvevői hamarosan válaszolni kezdtek: „Szia, a zászlóaljba akarok jelentkezni, mit kell tennem?" „Rzsaka. Gyertek, hekkerek – életünket és vérünket áldozzuk rá, hogy a házigazdát szolgáljuk." Voltak olyanok is, akik komolyabban vették az április 1-jei tréfát: végül is, Szevera volt az egyike azon kevés kiberbűnözőnek, aki a 1990-es években kezdte, és akkoriban nem kapták el.

Pjotr Levasov, aki a későbbiekben Szevera álnévvel illeti magát, Leningrádban született 1980 augusztusában. Fizika-matematika szakos gimnáziumot végzett, amely a szovjet matematikai iskolák tradícióját folytatta. Az iskolában rajongott a hekkerség iránt, és hamarosan olyan botnethálózatok létrehozójaként vált ismertté, amelyeket a spamek kiküldésére használnak, valamint ő volt a hamis antivírusok értelmi szerzője is. Ez utóbbiak „átvizsgálva" a számítógépet, a felhasználónak értesítést küldtek a feltárt problémákról, és a „gyógyításért" pénzt követeltek. Levasov-Szevera volt az alvilági orosz hekkerfórumokon a spamrészlegek moderátora, gyakran kötött össze egymással hekkereket, megismertette az újoncokkal a szakma alapjait, és segített botnetet építeni.

Amint azt az egyik, Levasov tevékenységét ismerő interjúalanyom elmondta, a 2000-es évek közepétől Szeverát hirtelen elkezdték a fórumok más tagjai beajánlani az államnak internetes segítségnyújtásra: először a csecsen terroristák, utána pedig az orosz ellenzékiek weboldalainak megtámadására. Erről Andrej Szoldatov és Irina Borogan újságíró is írt.[93] A csecsen terroristák azt is elmondták, hogy érkezett hozzájuk egy levél az „FSZB-s Szamuel" nevű hekkertől, amelyben azt ajánlotta, hogy felhagy a támadásokkal, ha teljesítik a feltételeit: „Egy kérdés ára 100 000 dollár.



Meg lehet egyezni. Bin Laden nem fog elszegényedni." Levasov támadásra szólította fel a hekkereket a svájci és a litvániai hostingcégek ellen, ahol helyet biztosítottak a *Kavkaz Center* nevű weboldal számára. Ugyanezekben az években, néhány hekker riportalanyom szerint, Levasov kezdte bérbe adni a saját botnethálózatait Kreml-barát ifjúsági mozgalmaknak.

2012 telén Levasov botnete bekapcsolódott az orosz választási kampányba: leveleket küldött szét[94] és a homoszexualitást emlegette Mihail Prohorov elnökjelöltsége kapcsán. A homofób oldalon ez negatív pírt jelentett. A levelekben egy olyan anyagra hivatkoztak, amelyet úgy tüntettek fel, mintha Prohorov-idézet lenne: „Minden ismerősöm számára régóta világos, hogy homokos vagyok."

Más hekkerek nemegyszer azzal gyanúsították Szeverát, hogy együttműködik a titkosszolgálatokkal, például, segít nekik kézre keríteni a CarderPlanet nevű fórum tagjait. Az egyik riportalanyom szavai szerint Levasov – az alvilági kiber más képviselőitől eltérően – egészen a 2000-es évek végéig folytatta az ICQ használatát, de őt nem tartóztatták le, bár a messenger ekkorra már a Mail.ru-hoz tartozott, és a titkosszolgálatok könnyen megszerezhették a hozzáférést.

Maga Szevera azt mesélte,[95] hogy 1999 óta foglalkozik spammel, önmagát „az internet egyik legéletképesebb spamkirályának" nevezte.[96] Egymillió reklámhordozó levélért kétszáz dollárt kért, egymillió phishing levélért ötszázat. Napi tizenöt megrendelés is befutott. „A tehetős kliensek iránt érdeklődöm, és aktívan ösztönzöm őket a nagy árengedményekkel. Minél nagyobb a rendelés volumene, annál nagyobb az árengedmény" – írta. Mint más kiberbűnözők, Levasov szinte soha nem működött Oroszországban, ezt elvi kérdésként kezelte: „Sorry, ez az én Hazám." Amikor 2014-ben megkezdődött a háború a Donyec-medencében, a hekker kijelentette, hogy 30 százalékos árengedményt vezet be az Ukrajnába, az Egyesült Államokba,

az EU országaiba és más, Oroszország ellen szankciókat életbe léptető államokba címzett küldeményeire. „Hogy az adott árengedményt megkaphassák, a rendelés kifizetéséig be kell mondani a következő jelszót: »Mentsük meg a Donyec-medence lakosságát a pederaszta elnöktől.«"

2017. április elején Levasov a feleségével és négyéves gyermekével Barcelonában üdült. Egyik éjjel az apartmanjukba az ajtót betörve behatolt a rendőrség, és mindenkit a földre kényszerített. Levasovot letartóztatták, és botnet létrehozásával vádolták.

Levasov felesége azt mondta,[97] a házkutatás alatt a titkosszolgálatok munkatársai minden elektronikus berendezést elkoboztak tőlük, és közölték, azért veszik őrizetbe a hekkert, mert „a vírus, amelyet állítólag a férjem hozott létre, kapcsolatban van Trump választási győzelmével". A feleség erre kijelentette, hogy a családjuknak soha nem volt „őrületes pénze", Levasov pedig egyáltalán nem hekker, a számítógépet alapvetően játékokra használja.

Barcelonából Madridba szállították Levasovot, itt állították bíróság elé, ahol kijelentette, hogy tíz évig dolgozott az Egységes Oroszország Pártnak, hogy információkat gyűjtsön az orosz ellenzékről. Levasov kijelentette, fél az Egyesült Államokba való kiadatástól: „Kínvallatásnak fognak alávetni, és még idén meg fognak gyilkolni, vagy én végzek magammal, [ők] információt akarnak szerezni az Egységes Oroszország Párt katonai jellegéről is."

Az Egységes Oroszország Párt tagadta, hogy együttműködött volna Levasovval, a külügyminisztérium pedig igyekezett elérni, hogy a hekkert ne adják ki az USA-nak, és azzal vádolták[98] az amerikai hatóságokat, hogy „alattomosan" akkor tartóztatnak le oroszokat, amikor azok külföldre utaznak. A minisztérium arra törekedett, hogy a hekkert Oroszországnak adják ki, azzal az indokkal, hogy 2014-ben egy szentpétervári kórház számítógépeit törte fel,[99] de a spanyol bíróság végül az amerikai kormány kérésének tett eleget. 2018 februárjában a hekkert átszállították az Egyesült Államokba.

Ott Levasovot egyáltalán nem az orosz állam hasznára végrehajtott feltörésekkel vádolták, hanem a Kelihos nevű botnet létrehozásával, amelyhez több mint százezer fertőzött számítógép tartozott. Az amerikai hatóságok úgy vélik, a botnetet nem csupán spamekhez, hanem DDoS-támadásokra, valamint a fertőzött eszközökről származó adatok ellopására is használják.

Oroszország amerikai nagykövetsége azt közölte, „rendkívül nyugtalanító Pjotr Levasov helyzete, aki újabb áldozata lett az amerikai titkosszolgálatok oroszok elleni, egész világra kiterjedő »vadászatának«". A diplomaták, akik meglátogatták a börtönben Levasovot, azt mondták, hogy szörnyen bánnak vele: „Az orosz állampolgárt egy kis méretű, kétszer két méteres magánzárkában helyezték el, ahonnan gyakorlatilag hiányzik a világítás. A cella folyamatos zajhatásnak van kitéve, amely a szomszéd helyiségekből származik. Ebből kifolyólag, illetve a párna és a matrac hiánya miatt Levasov meg van fosztva a teljes értékű alvástól. Ezenkívül megtiltották neki, hogy érintkezésbe lépjen más fogvatartottakkal, hogy sétáljon a friss levegőn, sőt még azt is, hogy telefonon felhívja az oroszországi rokonait.

Az Egyesült Államokban Levasov bűnösnek vallotta magát csalás, számítógépes védelem terén elkövetett bűnügyek, illetve személyes adatok ellopása miatt. Akár ötven év börtön is fenyegeti, az ítéletét 2019 őszén fogják kihirdetni.*

* Az ítélethirdetést elhalasztották. – *A szerkesztő megjegyzése.*

*III. rész*

# Hatalom

*19. fejezet*

# A KGB-s medvebocs

1989. június 3-án Németországban, egy Hannover melletti erdőben ismeretlen férfi összeégett holttestére bukkantak.[100] A tetem egy elhagyatott és poros autó mellett feküdt, amely úgy nézett ki, mintha már néhány éve ott állna abban az erdőben. Mellette üres benzintartály hevert. A férfin nem volt cipő – azt később sem találták meg.

A rendőrség nem sokkal utóbb közölte, hogy az elhunyt egy huszonnégy éves hannoveri lakos, Karl Koch. Eltűnését Koch főnöke jelentette be, amikor az alkalmazottja nem tért vissza a munkába ebédidő után. A rendőrség öngyilkosságnak vélte a halálát, és alighanem ez keltette fel az újságírók figyelmét, mivel Koch egy nagy port kavart bírósági eljárás szereplője volt. Azzal gyanúsították, hogy a KGB-nek dolgozik.

Koch egy hekkercsoport tagja volt, amely éveken át az amerikai védelmi minisztérium, a NASA és más amerikai intézmények rendszereit törte fel. A feltört számítógépekről letöltötték azokat a dokumentumokat is, amelyek hozzáférést biztosítottak a rendszerhez, amelyen keresztül Kelet-Berlinben KGB-alkalmazottaknak kábítószereket adtak el.

Koch általános iskolásként olvasta el a *The Illuminatus!* (Az illuminátus!) című könyvtrilógiát: ennek igen hatásos és fantasztikus szüzséje egy világméretű összeesküvésről szóló teóriába ágyazódik. Már számítógépes szakemberként Koch a Howard kapitány álnevet adta magának e regénytrilógia egyik hősének tiszteletére. Koch meg volt róla győződve, hogy a számítógépes hálózatok szintén azoknak

az illuminátusoknak a csapdája, akik titokban a világot irányítják, őrá viszont, mint Howardra is, egy másik bolygó lakói vigyáznak.

Koch, barátaival együtt, ahhoz az első nemzedékhez tartozott, amely már használta a személyi számítógépeket és a jelenlegire hasonlítani kezdő internetet. Az 1980-as évek elején a számítógépeket már nemcsak a hadászati vagy a programozói szükségletek miatt használták, hanem otthon is, például tanuláshoz, a családi költségvetés vezetéséhez, és természetesen az olyan videójátékokhoz, amilyen a *Space Invaders* vagy az *Arkanoid* voltak. 1981-ben az IBM kibocsátotta az első PC-jét, az Apple pedig az első Macintoshát. Megjelentek az olyan, jóval olcsóbb számítógépek is, mint például a ZX Spektrum, amelyeken el lehetett kezdeni a programozást. Ezekben az években jött létre a TCP/IP-adatcsere protokoll, valamint a DNS (tartománynévrendszer) és a világháló rendszere is – ezek mind a mai internet összetevői.

Ezzel egy időben nemcsak az első hekkerek, de az általuk létrehozott egyesületek is megjelentek. 1981-ben Németországban néhányan a Chaos Computer Clubba tömörültek, amelynek tagjai azt tervezték,[101] hogy az új digitális rendszerek segítségével megváltoztatják a társadalmat.

Koch szoros kapcsolatba került néhánnyal a Chaos Computer Clubhoz tartozó emberek közül. Egyik új ismerősének azt mondta, kigondolt egy módot az öngyilkosságra: atombombát kell gyártani, és a New York-i Világkereskedelmi Központ egyik tornyára felmászva fel kell robbantani.

Ugyanebben az időszakban, az 1980-es évek közepén, Koch nyilatkozatot tett közzé, amelyben megjósolta, hogy a közeljövőben informatikai háborúk indulnak a „lágy bombák", azaz a számítógépes vírusok felhasználásával. Találkozóin ismeretleneknek folyton azt ismételgette, hogy ő a jelenkori hekkerek legkomolyabbika és legtehetségesebbike.



Koch nem sokkal később megismerkedett a kamasz Pengóval, aki nagy rajongója volt William Gibson kiberpunk regényének, a *Neuromancnak*, amelynek hőse a számítógépes hálózatokról lopja az információkat. 1984-ben a tizenhat éves Pengo felhagyott a tanulással, és hátat fordított a barátainak, otthagyta a videójátéktermi munkáját is, hogy minél több időt tölthessen a számítógépével és a modemjével.

* * *

A hidegháború utolsó éveiben sokan előre megérezték a hamarosan bekövetkező változásokat, de az Egyesült Államok és a NATO országai formálisan még mindig a Szovjetunió ellenségei maradtak. 1986-ban Koch, Pengo és barátaik arról ábrándoztak, hogy a feltörésekkel sok pénzt keresnek – és elhatározták, hogy a keleti blokk országainak javára számítógépes kémtevékenységbe kezdenek. Csoportjukat Equalizernek nevezték, arra utalva, hogy szerintük a szovjet hatalomnak eladott hadi és tudományos információkkal egyenlővé teszik a szovjetek esélyeit a nyugati országokkal szemben, s az így létrejövő egyensúly révén az egész világon megszilárdítják a békét.

1986 szeptemberében a kelet-berlini Unter der Lindenen található orosz nagykövetség épületébe megérkezett a hekkercsoport egyik tagja, Peter Karl. A bejáratnál azt mondta az őrnek, hogy beszélni szeretne egy ügyben valakivel a KGB-től. Az őr arra kérte, várjon, majd fél óra elteltével megérkezett egy férfi, és azt kérdezte a hekkertől, mi járatban van. Karl elmagyarázta, hogy ő és barátai hozzá tudnak férni a világ legtitkosabb adatokat tartalmazó rendszereihez, és a Szovjetunió rendelkezésére tudják bocsátani azokat a technológiákat, amelyek segítenek neki felülmúlni a nyugatot. Erre az alkalomra a hekkerek előkészítettek a KGB számára egy „demó csomagot": megszerezték a hozzáférést az amerikai védelmi minisztérium információs rendszeréhez, és lemezekre másoltak néhány titkos dokumentumot, például az összes, addig a pillana-

tig az USA területén birtokolt számítógép jegyzékét. Miután Karlt végighallgatta, a KGB munkatársa biccentett és távozott, de tíz perc elteltével egy másik férfi jött ki, aki Szergejként mutatkozott be. Karl és csoportja tagjainak emlékezete szerint Szergej nem igazán értette, hogy mit jelent a „hekker" szó, de felajánlották neki, hogy elhozzák az ellopott dokumentumok egy példányát, amit elküldhet Moszkvába szakértői vizsgálatra. Maguk között a hekkerek a KGB munkatársát Teddy Bear gúnynévvel illették.

Az 1980-es évek végére a szovjet titkosszolgálatoknak még nem sikerült kinevelniük a számítógépes védelemben és támadásban jártas saját szakembereiket. Mindent összevetve, ez a találkozás volt az első kísérlet a hekkerekkel való együttműködésre, és a KGB munkatársai még nem nagyon voltak tisztában az ebben rejlő lehetőségekkel. Amikor a hekkercsoport egyik tagja szemináriumot tartott a hekkerségről a szovjet titkosszolgálatoknak, Szergej azt mondta, őt ez nem érdekli.

A következő találkozók a KGB-vel heti rendszerességgel zajlottak. A hekkerek megmutatták Szergejnek a számítógépek listáját, amelyekhez meg tudták szerezni a hozzáférést, Teddy Bear pedig válaszul közölte munkaadóinak a kívánalmait: szükségük van a rádiótechnikáról, a nukleáris fegyverekről és a stratégiai védelmi kezdeményezésről (SDI) szóló dokumentumokra, vagyis annak a világűrbe telepített rakétaelhárító, akkori közkeletű nevén csillagháborús programnak a részleteire, amelyet az Egyesült Államok elnöke, Ronald Reagan 1983-ban hozott nyilvánosságra. A KGB-t tulajdonképpen bármilyen dokumentum érdekelte, amely az USA védelmi minisztériumának számítógépeiről származott, ezen kívül pedig az amerikai operációs rendszerek fejlesztéseire vonatkozó információk is.

Az idő nagy részében az egymással barátságban álló hekkerek egyszerűen „szörföltek" a hálózatokon, és érdekes információkat kerestek. A rendszerekbe behatolva a



*nuclear*, az *SDI*, a *star wars*, a *missile** szavakra kerestek rá. Azon dokumentumok közül néhány, amelyeket a hekkerek a KGB-nek továbbítottak, az akkori idők internetén egyszerű kereséssel megtalálható volt, a szovjet tisztviselők mégis fizettek[102] értük: a Pentagon szó számukra mágikus volt.

A következő találkozókon, amikor a hekkerek még semmit sem szállítottak, Szergej kifizetett nekik hatszáz német márkát (azaz háromszáz dollárt), és ajándékokat adott nekik: kaviárkonzerveket, szép öngyújtókat és hasonlókat. Egyiküknek odaadta a barátnőjéről készült fotót, hogy azt mutassa meg a rendőrségnek, ha megkérdeznék tőle, kihez is utazik olyan gyakran Kelet-Berlinbe.

A hekkerek átadták a hozzáférést a KGB-nek a Pentagon és a NASA adatbázisaihoz, a Los Alamos-i nukleáris laboratóriumhoz, valamint Nyugat-Németország, Franciaország, Japán és Nagy-Britannia űr- és nukleáris infrastruktúrájáról szóló anyagokat. A hekkercsoport többek között feltörte a genfi CERN nukleáris kutatóközpontjának rendszerét is. Az adatok átadásáért a KGB-től néhány százezer dollárt kaptak.

1988-ban az USA titkosszolgálatai – Clifford Stoll programozóval közösen, aki először észlelte a behatolást annak az amerikai egyetemi könyvtárnak a számítógépes rendszerébe, ahol ő dolgozott – kiderítették, hogy a hekkerek a katonai intézmények harminc számítógépéhez szerezték meg a hozzáférést. A feltörők nyomába eredtek, és a Német Szövetségi Köztársaság titkosszolgálatai különböző német városokban hamarosan letartóztatták a hekkereket. A tárgyalás időszakában viszont szabadlábon védekezhettek.

Koch rejtélyes halálától eltekintve a tárgyalás nyugodt körülmények között zajlott. A legfőbb tanúvá a hekkercsoport tagjai közül Pengo vált. Részletes vallomást tett, és vádalkut kötött. A kamasz amnesztiát kapott, más hekke-

* Az angol szavak jelentése: nukleáris, SDI = *Serial Digital Interface*, Soros Digitális Interface, csillagháború, rakéta.

reket feltételesen szabadon bocsátottak, és pénzbüntetést kaptak. Az ügyet megvizsgálva a bíróság rájött, hogy a szovjet titkosszolgálatok egyszerűen nem értették, milyen lehetőségeket kínáltak nekik a hekkerek. Mindazonáltal a német ARD tévécsatorna a hekkerek tevékenységét úgy értékelte,[103] mint a legkomolyabb kémügyet 1974 óta, amikor kiderült, hogy a Német Szövetségi Köztársaság kancellárjának egyik tanácsadója keletnémet kém volt.

Koch ismerősei nem öngyilkosságnak vélték a halálát: egyiküket[104] az lepte meg, hogy a holttest körül a fű épp egy jól körülhatárolható körben égett ki, másokat[105] az, hogy a hekker egy benzintartállyal nagyjából hetven kilométert utazott otthonról az erdőbe, ahelyett, hogy ennél jóval egyszerűbb módon végzett volna magával.

Idővel Koch története sajátos hekkerlegendává változott: a fórumokon olykor „nagy harcosnak" nevezik.[106] A német hekkercsoport történetét az 1990-es években John Markoff mesélte el *Cyberpunk* (Kiberpunk) című könyvében. Ez azon ritka, hekkerekről szóló könyvek egyike volt, amely oroszul is megjelent, és az interneten is terjesztették az évtized közepén-végén. Ebben az időben bárki, aki a kiberalvilágban dolgozott és az állammal való együttműködésen gondolkodott, ismerhette ezt a történetet.

*20. fejezet*

## Patrióta hekkerek

Huszonöt évvel Karl Koch rejtélyes halála után a KGB egykori munkatársa, Vlagyimir Putyin, aki éppen azokban az években dolgozott a Német Demokratikus Köztársaságban, amikor hivatala együttműködött a hekkerekkel, patrióta hekkerekről kezdett beszélni. Erre történetesen az a kérdés adott alkalmat, amelyet a 2017-es Pétervári Gazdasági Fórumon egy német újságíró tett fel Oroszország elnökének.

– *Németországban elég idegesen reagáltak az Oroszország felől érkező hekkertámadások hírére és arra, hogy az orosz hekkerek manipulálhatják akár a választásokat is* – mondta Peter Kropsch, a legnagyobb német hírügynökség, a DPA igazgatója. – *Mit gondol ön erről?*

– *A hekkerek szabad emberek!* – válaszolta Putyin. – *Csakúgy, mint a művészek. Ha reggel jó hangulatban ébrednek, egész nap csak festenek. Mint a hekkerek: ha ébredés után azt olvasták, hogy történik valami a nemzetközi színtéren, és ha elég hazafias hangulatban vannak, akkor úgy érzik, az a helyes, hogy ha részt vesznek a küzdelemben azok ellen, akik negatív véleményt fogalmaznak meg Oroszországról. Elvileg ez lehetséges. Állami szinten ezzel nem foglalkozunk, és ez a legfontosabb. Azt is el tudom képzelni, hogy valaki úgy építi fel egy támadás láncszemeit, hogy abból arra lehessen következtetni, hogy a támadás Oroszországból indult. Ezt ma már a modern technológia lehetővé teszi, és nem nehéz megoldani.*

Az orosz elnök nyilatkozata némiképp emlékeztetett Donald Trump azzal kapcsolatos kommentárjára, hogy orosz hekkerek lehettek azok, akik kísérletet tettek az ame-

rikai választások befolyásolására. Trump közölte, hogy az amerikai Demokrata Párt struktúrájába betörni „bármelyik száznyolcvan kilós hekker képes lehet, aki az otthonában a díványon ül".

„Szilárd meggyőződésem, hogy semmiféle hekker nem tudja végzetesen befolyásolni egy másik országban folyó választási kampány végkimenetelét – tette hozzá Putyin, miközben a szívéhez szorította a kezét. – Ez nem befolyásolja a választók és a nép tudatát, a választás végeredményére pedig semmiféle információ sem hat."

Putyin retorikája az évek során nem változott, függetlenül attól, milyen bizonyítékok támasztják alá a vádat, hogy a hekkertámadásokat a Kreml szervezi. 2016-ban, amikor ezek a vádak még éppen csak körvonalazódtak, az elnök szinte ugyanezekkel a szavakkal reagált.[107] „Tudják, hány hekker van manapság? Egyébként annyira precízen, annyira finoman működnek, hogy csak a kellő helyen és a kellő időben hagynak nyomot maguk után – pontosabban ez még csak nem is a saját nyomuk, hiszen a tevékenységüket valamely más területről, más országokból származó, más hekkerek tevékenységével álcázzák – mondta Putyin. – Állami szinten ezzel valóban nem foglalkozunk."

Csakhogy ez nincsen egészen így. Az utóbbi években Oroszország aktívan foglalkozik a kiberfegyverkezés és a kibervédelem rendszerének a kidolgozásával, és toboroz is hekkereket különböző feladatokra. A patrióta hekkerek, akik sikerrel segítik az államot geopolitikai célkitűzéseinek elérésében háborús konfliktusok idején, már tíz évvel ezelőtt elkezdték a tevékenységüket.

* * *

1999 augusztusában és szeptemberében Moszkvában és Volgodonszkban felrobbantottak néhány lakóházat: háromszázhét ember meghalt, körülbelül ezerhétszázan megsebesültek. A történtekért a csecsen terroristákat vádolták, hiszen szintén 1999 augusztusában katonai különítmények Samil Baszajev vezetésével megkezdték a hadműveleteiket Dagesztán területén, hogy felszabadítsák a régiót a „máshitűek megszállásától".



Az orosz csapatok hamarosan blokád alá vonták Csecsenföld határait, és szeptember 30-án (egy héttel az után, hogy Borisz Jelcin elnök aláírta a parancsot a „terrorellenes művelet", azaz a KTO végrehajtásáról) behatoltak a köztársaság területére. A „művelet", amelyet hivatalosan nem is neveztek háborúnak, a következő tíz évben folytatódott: formálisan a KTO-t csak 2009 áprilisában vonták vissza.

A második csecsen háború volt az első olyan konfliktus, amelyben az orosz hekkerek az állam oldalára állva ténylegesen harcoltak az ellenséggel. Míg a lakóházak felrobbantása után az orosz városokban emberek a lépcsőházak bejáratainál őrködtek és figyelték a gyanús idegeneket az alagsorokban, addig mások úgy döntöttek, ők is aktívan felveszik a harcot az ellenséggel szemben – de úgy, hogy nem hagyják el a házukat és városukat.

A Tomszki Műszaki Egyetem egy hallgatói csoportja megszervezte[108] a „szibériai hálózati brigádot". A csapat DDoS-támadásokat intézett csecsen harcosok weboldalai ellen, ahol híreket és interjúkat közöltek. Egyébként a kiberaktivisták már azelőtt megkezdték a működésüket, mielőtt a konfliktus az aktív szakaszához érkezett volna. 1999. augusztus 1-jén a kavkaz.org nevű weboldal főoldalán posztoltak[109] egy karikatúrát, amely Mihail Lermontov költőt ábrázolta – álcában, kezében egy Kalasnyikovval. „Itt volt Misa – közölte az orosz zászló színeiben úszó aláírás. – Ezt a terroristák és gyilkosok által működtetett weboldalt az orosz emberek nagy számú kérésére zárták be."

A brigád tagjai leveleket küldtek amerikai hostingcégeknek is azzal a kéréssel, hogy szüntessék meg szolgáltatásaikat terroristák részére. 2001. november 17-én a szervezet vezetője felhívást intézett[110] az amerikai média és az USA Külügyminisztériuma számára:

*Az XO Communications Inc. nyújt tárhelyszolgáltatást annak*

*a »Kavkaz-Centr« nevű információs ügynökségnek, ami olyan személyek tulajdonát képezi, akiket az Önök országában is nemzetközi terroristaként tartanak számon. Az adott weboldalt nem csak arra használják, hogy a nemzetközi terrorizmus elleni küzdelemben tett világméretű erőfeszítéseinkre vonatkozó lejáratő anyagokat tegyenek közzé, hanem új harcosokat is toboroznak, illetve a terroristák számára pénzt gyűjtenek.*

Egy hónap múlva a hostingszolgáltatást megtagadták a Kavkaz Centertől, amely grúz szerverekre költözött át (később a weboldalnak tovább kellett költöznie[111] Észtországba, Lettországba és Finnországba).

2002-ben a brigád patrióta hekkerei ismét feltörték a Kavkaz Center weboldalát, és a főoldalán hagytak egy közleményt.

*„Kihúztuk a Gavgav Center* bűzös pofájából a méregfogat, így a csecsen terroristák fészke felett csend honol. Udugov belefullad a káromkodásba [Movladi Udugov, ebben az időben a Kavkaz Center vezetője és a Csecsen Köztársaság hírközlési minisztere volt]. A hegyekben elhallgatott a banditák automata fegyvere. Nem küldött a csecsen zsoldosnak pénzt a ravasz arab. Szomorú a gonosz tálib Afganisztánban. Hogyha holnap betömitek ezt a pofát, a világ nyugodtabb és biztonságosabb lesz."*

A brigád arra is nyíltan felszólította a kollégákat, hogy a harcosok segélyforrásait is támadják meg: „a legjobbaknak járó elismerés, amikor a bátyuskáid rajonganak érted az online cégből, a holnap pedig boldog napfényben úszik majd." Néhány hónap múlva az orosz nyelvű hekkerek tömegesen terjeszteni kezdték[112] a *Masyanya* vírust, amelyet az az idő tájt népszerű, interneten látható animációs film tiszteletére neveztek el így. Ártalmatlan volt a felhasználók számára, de a vírus parancsára fertőzött számítógép a Kavkaz Center elleni DDoS-támadások résztvevőjévé vált.

* A Kaukázus, azaz oroszul a Kavkaz szót itt a hekkerek direkt változtatták meg Gavgavra, mintegy gúnynevet adva így a központnak. – *A fordító megjegyzése.*



A Kavkaz Center vezetője, Movladi Udugov meg volt róla győződve,[113] hogy a hekkerek akciói mögött az FSZB áll. Tomszkban az FSZB nyíltan beszélt arról,[114] hogy a „szibériai hálózati brigád" nem sérti meg az orosz törvényeket, tagjainak tevékenysége pedig nem más, mint „állampolgári érzületük kifejezése, ami tiszteletet érdemel" – holott valójában ekkor már hatályban volt a büntető törvénykönyv 272. cikkelye a számítógépes információhoz való jogtalan hozzáférésről.

Egy hónappal később, 2002. október 23-án csecsen terroristák elfoglalták a moszkvai Dubrovka Színházat, ahol a *Nord-Oszt* című musicalt mutatták be. A terroristák weboldalait ekkor ismét feltörték. Ezután a „szibériai hálózati brigád" beszüntette akcióit, s hogy a tagjai mivel foglalkoztak az ezt követő években, az nem ismeretes.

* * *

2005-ben a patrióta hekkerek történetében új korszak kezdődött: az erre szakosodott fórumokon ekkor jelentek meg az egyesülésre irányuló felhívások, hogy megtámadhassák a kritikus infrastruktúrákat is.

Az egyik, aki ezeket a posztokat megosztotta, Pjotr Szevera volt, a spam királya, akit később, 2017-ben Spanyolországban tartóztattak le. Például ő ajánlotta az alvilági kibermozgalomban részt vevő társainak, hogy lépjenek be a Civil Antiterrorba, abba a társaságba, amelyet 2005 tavaszán alapított[115] néhány patrióta hekker. Ők közzétettek egy kiáltványt is arról, hogy a 21. században a legfontosabb fegyver az információ. „A célunk, hogy elzárjuk a hozzáférést azokhoz a forrásokhoz, amelyek fals információkat terjesztenek a terrorizmusról és a terroristákról, megalapozatlanul propagálják tevékenységük helyességét – közölték. – A terrorista szervezetek megengedhetnek ma-

guknak kiváló szakembereket, akik biztosítják forrásaik védelmét. Tiszteljük a profizmusukat, de nem értjük, hogyan adhatják el a saját lelkiismeretüket." A tagok ugyanazokkal a módszerekkel tevékenykedtek, mint az elődeik, azaz DDoS-támadásokat hajtottak végre.

Egy hónappal később napvilágot látott[116] egy másik hasonló projekt is: az Internet Underground Community vs Terrorism (Az internet földalatti közössége a terrorizmus ellen). Ez a weboldal fekete és sötétkék színekben játszott: a weboldal tetején egymással szemben állt a hekker és a ghutrát viselő alak (férfifejkendő, amely az arab országokban elterjedt). A projekt létrehozói felhívták a figyelmet,[117] hogy DDoS-szakembereket keresnek, és tagadták, hogy kapcsolatban állnának az orosz hatalommal és a titkosszolgálatokkal. Azt hangoztatták, hogy a projektet olyan emberek találták ki, akik a törvény „túloldalán helyezkednek el". A weboldal „program" nevű részében posztolták a DDoS-támadáshoz szükséges eszközöket, és ugyanide tették ki azt a dicsőségtáblát is, amelyen megjelölték a megtámadott forrásokat és az időtartamot, ameddig ezek nem tudtak működni.

A terroristák 2005. októberi, Nalcsikot ért támadása után[118] a hekkerek nemcsak a Kavkaz Centert, hanem azokat a tömegmédiumokat is megtámadták, amelyek szerintük hamisan beszéltek a terroristák tevékenységéről: az *Ekho Moszkvit*, a *Novaja Gazetát* és a Ragyio Szvobodát. Még egy hónap elteltével feltörték Eduard Limonov Nemzeti Bolsevik Pártjának weboldalát is (amely párt Oroszországban be van tiltva). A legfelsőbb bíróság éppen a támadást követő napon tiltotta be a Nemzeti Bolsevik Párt nemzetközi csoportját.

Ez után a DDoS-támadás után az ellenzéki és tiltakozó weboldalak létrehozása egyre gyakoribbá vált. 2007 tavaszán nemzetközi konfliktussá dagadt egy vita, amely a második világháborús szovjet katonai emlékmű Tallinn központjából egy katonai temetőbe való átszállítása ügyében keletkezett. Az orosz külügyminisztérium tiltakozójegyzéket küldött Észtországnak, Moszkvában pedig az észt nagykövetség épülete előtt a Mieink nevű Kreml-barát mozgalom csapatai vonultak fel.

A hekkerek ebben a pillanatban támadták meg Észtország köztársasági elnöke, miniszterelnöke, valamint állami hivatalok és bankok weboldalát: ez utóbbiak a DDoS-támadás miatt néhány hétig nem tudtak működni. A kormányzó Észt Reformpárt főoldalán egy kiáltvány jelent meg, és a hekkerek felszólították Andrus Ansip pártelnököt és észt kormányfőt, hogy nyilvánosan olvassa fel. A kiáltvány bocsánatkérést tartalmazott Észtország orosz lakosságától, és a kötelezettségvállalást arra, hogy az emlékművet visszaállítják eredeti helyére. Az egyik megtámadott banknak a helyreállítás körülbelül tízmillió euróba került.[119] Az Elliott School of International Affairs a támadásokat az „első kiber-világháborúnak" nevezte a jelentésében.[120]

A támadás megszervezéséért a felelősséget a „Mieink" mozgalom biztosa, Konsztantyin Goloszkokov vállalta magára.[121] „Nem nevezném ezt támadásnak, sokkal inkább kibervédelemnek – mondta.[122] – Az észt rezsim leckét kapott." Az USA titkosszolgálatai úgy vélik,[123] a különböző botnettámadásokat Pjotr Szevera irányította.

Nagyjából ugyanebben az időben Anton Moszkal pétervári programozót felhívta egy ismeretlen. Amint arról Andrej Szoldatov újságíró beszámolt,[124] a férfi úgy mutatkozott be, mint az FSZB Nemzeti Antiterrorista Bizottságának munkatársa. Megkérdezte, vajon valóban Moszkal-e a tulajdonosa a Civil Antiterror című weboldalnak. A weboldal valójában nem őhozzá tartozott, Moszkal csak ennek a tükrét hozta létre a saját blogján. Az FSZB munkatársa „a programozóval beszélgetést folytatott a patriotizmusról és a terrorista weboldalak elleni harcról". Amikor megtudta, hogy nem annak telefonált, akinek szeretett volna, megkérdezte Moszkaltól, hogyan léphetne kapcsolatba azokkal a hekkerekkel, akik a projekten dolgoznak.

*21. fejezet*

## Megfékezni Grúziát

2008. augusztus 8-án Leonyid Sztrojkov hekker, aki a posztjait leggyakrabban ROiDként írta alá, ült a habarovszki lakásában, sörözgetett, és a Basorg című humoros weboldalt olvasgatta. Egyszer csak a tévé rendkívüli híradással jelentkezett: azt közölték, hogy grúz csapatok lőni kezdték Dél-Oszétia fővárosát, Chinvalit. (Dél-Oszétia formálisan Grúzia része volt, de a régió vezetésének hosszú évek óta húzódó konfliktusa volt Tbiliszivel.)

2008. augusztus 8-a éjjelén tehát Grúzia lőni kezdte Chinvalit. A tüzérségi támadás előtt már mindkét oldalról lövöldöztek egymásra a határ menti falvakban. A grúz csapatok elfoglalták a várost. Az orosz tévécsatornákon szinte azonnal ezres nagyságrendű áldozatról és az „oszét nép genocídiumáról" kezdtek beszélni. Ezt követően a konfliktus viharos gyorsasággal Grúzia és Oroszország ötnapos háborújává fejlődött. A Vlagyikavkázból odaérkező orosz csapatok kiűzték a grúz katonákat Chinvaliból. Az orosz nyomozóbizottság adatai szerint a 2008. augusztusi események alatt százhatvankét dél-oszétiai lakos és ötvennégy orosz katona vesztette életét. Grúzia részéről egyes források szerint a halottak száma elérte a háromszázkilencvenhetet (nagy többségükben civilek voltak), és grúzok ezrei kerültek menekülttáborokba.

A hallottak hatására a tapasztalt hekker, Sztrojkov (aki 2006-ban például részletesen beszámolt arról,[125] hogyan tört fel egy online bankot) tanulmányozni kezdte a grúz kormányszerveket és a tömegmédiát: támadásokra alkalmas réseket keresett a védelmükön. Hamarosan fel is törte



néhány grúz médium weboldalát. Ezután az állami oldalakra fordult a figyelme. Nemsokára Miheil Szaakasvili grúz elnököt Hitlerként ábrázoló fotók jelentek meg a grúz parlament internetes oldalán. *„És ugyanúgy végzi majd ő is..."* – szólt a kommentár. – *Hacked by South Osetia Hack Crew.* [Meghekkelte a Dél-Oszétia Hekker Legénység.]"

„Egyetlen nagy horderejű esemény sem mehet végbe a tömegmédia nélkül: a média felületei arra használják az internetet, hogy a történéseket a saját látásmódjuk szerint közvetítsék, és kizárólag azt közlik, amit akarnak, vagy azt, amit súgnak nekik – írta később Sztrojkov. – Az orosz és a grúz/nyugati kiadványok egymáshoz képest abszolút ellentétes nézetei arra késztettek, hogy mélyebbre ássam magam a témába, annak minden következményével együtt." Sztrojkov a Grúzia elleni támadásáról részletesen beszámolt a *Hekker* című folyóiratban, közölvén, hogy a „kiberháborúk szerves részévé válnak a reális, vérontással járó eseményeknek".

Nem Sztrojkov volt az egyetlen hekker, aki „mélyebbre ásott a témába". Augusztus 9-én, egy nappal azután, hogy Oroszország Grúzia területére vezényelte csapatait, elkészült a stopgeorgia.ru nevű weboldal. Itt közzétettek egy listát[126] grúz weboldalakról, amelyeket megtámadni javasolnak, valamint hivatkozásokat tettek közzé az ehhez szükséges programokról, illetve tanácsokat nyújtottak a kezdő hekkereknek. A weboldal fórumán körülbelül harminc állandó tag volt jelen, alapvetően olyanok, akik hitelkártyacsalással keresték a kenyerüket. A felhívások a projektben való részvételre a *Hekker* portálján és más, a hekkerek érintkezését szolgáló felületeken jelentek meg, mint amilyen az exploit.in, a zloy.org, vagy a web-hack.ru.

A weboldal létrehozói „az orosz hekker-underground képviselőiként" mutatkoztak be. „Nem tűrünk el semmiféle provokációt Grúzia részéről – közölték a kiáltványukban.[127] – Szabad világban akarunk élni, agressziótól és hazugságtól mentesen létezni a hálózati térben." Ígéretet tettek arra,

hogy „addig fogják támadni a grúz erőforrásokat, amíg a helyzet meg nem változik", és segítségül hívták „mindazokat, akiknek nem közömbös a grúz politikai weboldalak hazugsága". A stopgeorgia weboldalon megjelent[128] egy lista a támadás „elsőrendű céljairól". Ezt követően szűnt meg működni a grúz elnök, a parlament, a belügyminisztérium és a védelmi minisztérium weboldala.

Ezekben a napokban történtek[129] kibertámadások orosz erőforrások ellen is: megtámadták a *RIA Novosztyit* és más orosz és oszét médiumokat is. A *Russia Today* weboldala a DDoS-támadás következtében körülbelül egy órán át nem működött. Valaki létrehozott egy weboldalt, amely úgy nézett ki, mint az oszét hírügynökség oldala, és tele volt álhírekkel.

A hekkerfórumokon az Észtország és Grúzia elleni támadásokat alapvetően helyeselték: „riszpekt az embereinknek", „szükség van az észt weboldalak elleni DDoS-támadásra és az Oroszországgal szembeni propagandájuk eltorzítására", „A fő szempont a hatékonyság. Mit számít, hogy aljasság vagy nem? Különösen háborús időben".

A stopgeorgia a háború után is tovább működött. Amikor 2009 decemberében a grúz hatóságok Kutaisziban lebontották a harci dicsőség emlékművét (a szovjet katonák emlékműve helyén kívánták felhúzni a parlament épületét), a hekkerek ismét bedöntötték a grúz állami weboldalakat. „Nem tűrjük a történelmi örökségünk megsemmisítését és annak a kísérletét, hogy az egykori Szovjetunió népeit egymás ellen uszítsák – írták közleményükben az egyik hekkerfórumon. – Fellépünk népeink békéje és barátsága érdekében, nem hagyjuk, hogy nacionalista viszályt szítsanak azok között, akiknek a történelmét örökre a barátság kötelékei fűzik össze."

Későbbi elemzők arra jutottak,[130] hogy a stopgeorgia.ru a Naunet internetszolgáltatóra volt bejegyezve, amely azután visszautasította a bűnüldöző szervek kérését, hogy adják ki a tulajdonosok adatait. A Spamhaus nevű szervezet régóta feketelistára vette a céget amiatt, mert felületet biztosít spammereknek és kiberbűnözőknek. A Naunet-csoport épülete nincs messze a Moszkva központjában elhelyezkedő Belorusz vasútállomástól: a netszolgáltató az épületen az Etalon kutatóintézettel osztozott, egy olyan, államhoz közel álló vállalattal, amely informatikai védelmi rendszerek gyártásával foglalkozik. 2015-ben az Etalon a Rosztech részévé vált, azaz annak az állami társaságnak a részévé, ahol Vaszilij Brovko dolgozik, akit a DDoS-támadások végrehajtásához szükséges programok és berendezések érdekeltek.

A stopgeorgia.ru-ra történő regisztrációhoz szükséges adatok mellett egy postafiók és egy telefon is megjelent a kártyások felületén – ezek egy bizonyos Andrej Uglovatijhoz (több mint valószínű, hogy ez a kitalált neve volt) tartoztak, aki lopott hitelkártyák adatállományával, valamint hamis útlevelekkel és vezetői engedélyekkel kereskedett.

A stopgeorgia.ru IP-cím a Steadyhost nevű kis társaságé volt, amely a Horosevszkij út 88. alatt található, Moszkvának azon kerületében, ahol szinte minden épület a hírszerző főigazgatósághoz (a GRU-hoz) tartozik. A szomszédos épületben, a 86-os számú házban a védelmi minisztérium 6-os számú kutatóintézete működik, amely katonai-műszaki információkkal és a külföldi államok katonai potenciáljával foglalkozik, korábban pedig a GRU-nak volt alárendelve. A helyi lakosok ezt a háromemeletes épületet, amely az 1930-as években épült, „Pentagonnak" nevezik, nem annyira a formája, mint inkább a titkossága miatt: e kutatóintézet munkatársait úgy jellemezték,[131] mint „a GRU legjobban informált embereit", az intézmény vezetője pedig Oroszország Biztonsági Tanácsának tagja.[132]

Néhány orosz nyelvű hekker elmondása szerint az orosz titkosszolgálatok éppen a Grúziában történt események idején és azt követően kezdtek szisztematikusan együttműködni a hekkerekkel. Azóta rendszeresen vonják be őket a munkába, néha önként, néha kényszerrel, büntetőeljárással fenyegetve őket.

Amint azt egyik interjúalanyom elmondta, a titkosszolgálatok jobbnak találják, ha nem tartanak státusban annyi műszaki szakembert, inkább státuson kívüli munkatársakat toboroznak: feltörésekkel és bankkártyacsalással kapcsolatos büntetőügyek keretében találnak rájuk, illetve az alvilág fórumain keresik fel őket. A Kaspersky Lab vizsgálati ügyosztályának korábbi feje, Ruszlan Sztojanov, aki sokszor dolgozott az FSZB-vel, nyíltan figyelmeztetett, hogy az ilyesfajta együttműködés veszélyes. „Hatalmas kísértés ez »a döntéseket elfogadó emberek számára«, hogy az orosz kiberbűnözés kész megoldásait használják fel a geopolitikát befolyásoló célokhoz – írta nyílt levelében[133] Sztojanov, akit 2017 januárja óta a lefortovói büntetés-végrehajtási intézetben tartanak fogva hazaárulás vádjával. – A legrosszabb forgatókönyv az, ha más országokban a kiberbűnözőket felmentik a lopott pénz miatti büntetés alól, kémkedésért cserébe. Ha ez megtörténik, a »hazafias tolvajok« egész sokasága jelenik meg. Ezek a félig legális hazafias csoportok jóval nyíltabban tudják befektetni a lopott tőkét a legkorszerűbb trójai programok létrehozásába, Oroszország pedig ily módon hozzájut a legmodernebb kiberfegyverzethez." Az ilyen patrióta csoportok szolgáltatásait a titkosszolgálatok már tíz éve használják.

Az, hogy mivel foglalkozott Leonyid Sztrojkov a grúz eseményeket követően, nem ismert; jelenlegi VKontakte-oldala alapján Sztrojkov szereti álcázni magát, és odavan a vadászatért. Kérdéseimre nem válaszolt. A közösségi hálón a hekkernek harminchat barátja van, a legtöbben Habarovszkból valók, ahol Sztrojkov korábban élt. A kivétel Dmitrij Dokucsajev, az FSZB munkatársa, aki hekkerkörökben Forb néven ismert. Dokucsajev volt az egyik első olyan hekker, aki állandó munkára szegődött a titkosszolgálatokhoz 2016-ban, és lehetséges, hogy kifejezetten az amerikai Demokrata Párt infrastruktúrája elleni támadásokhoz toborozták. (Dokucsajevről részletesebben a 31. fejezetben lesz szó.)

*22. fejezet*

## Hekkerek a liberálisok ellen

A következő években a patrióta hekkerek áttértek a belső „ellenségekre". 2013 tavaszán a Homjacski* nevű szervezet a legtöbb liberális médium weboldalát megtámadta, mert a hekkerek véleménye szerint megsértették május 9-e emlékét. „Ma a győzelem napja van, és ezen a napon különösen szeretnénk, hogy azoknak az embereknek az emlékét, akik az életüket adták a hazánkért, semmivel se sértenék meg, ne legyen lehetséges semmiféle kitaláció és a tények elferdítése. Ebből kifolyólag az elektronikus média egy sor weboldala ma nem működik" – közölték a hekkerek. Az általuk szervezett DDoS-támadások szakemberek szerint a legnagyobbak voltak az orosz internet történetében. Az orosz rendőrség nem reagált a támadásokra, ki sem vizsgálta azokat.

A Homjacskit szentpétervári egyetemisták alkották, a csoport egyik vezetője valószínűleg Makszim Bolonkin volt,[134] aki programozóként végezte el a műszaki főiskolát. Ugyanabban az évben a Kreml-barát ifjúsági mozgalmak Szeliger-tónál rendezett fórumán, egy *Homjacski* feliratú futballtrikót ajándékozott az orosz parlament küldöttjének. Szervezete hamarosan elnöki támogatást kapott[135] hétmillió rubel értékben, hogy létrehozzon „egy összorosz ifjúsági pozitív információs felületet".

A hekkereket nemcsak a „liberális" média érdekelte, hanem az ellenzéki politika is. 2012. június 25-én éjjel Alek-

* A szervezet neve „kis hörcsögöket" jelent. – *A fordító megjegyzése.*

szej Navalnij Twitter-oldalán a következő közlemények jelentek meg: „Csubakka, én itt eldöntöttem, hogy vallomást teszek", „Becsaptam magát, Csubakka, valójában az Egységes Oroszország Pártnál szívtam, és ezért helyet adtak nekem az Aeroflot igazgatótanácsában, meg ilyenek", „Homjacski, ebanyije baranyi,* becsaptam magukat, Putyinnak dolgozom, Belkovszkijtól kapom a lóvét, ne sértődjenek meg rám". „A szektát én magam eresztem széjjel, a pénzt nem viszem önöknek vissza, mert szükségem van rá, hogy Mexikóba mehessek, és mindenki elmehet a..." „Nyugodjék meg, homjacski, nyugodjék meg, és fogadja el a szörnyű igazságot..." „Engem senki nem tört fel, egyszerűen úgy határoztam, hogy megmondom önnek végül az igazságot, de megértem, hogy milyen nehéz most önnek..."

Navalnij követői azonnal rájöttek, hogy a politikus Twitter-fiókját feltörték, maga Navalnij pedig azt feltételezte, hogy ez azon számítógépeken és az iPadjeken történt, amelyeket nem sokkal korábban koboztak el a nála tartott házkutatás során. Egyébként a politikus azt mondta, húsz perccel azután megváltoztatta a jelszavát, hogy elvették tőle a technikai felszerelését.

A felelősséget egy Hell nevű hekker vállalta magára, egy anonim aktivista, aki egyebek mellett hisz a teljes világot átfogó zsidó összeesküvésben. A híresség fiókjainak feltörését még a 2000-es években kezdte, amikor a vezető orosz közösségi háló a Zsivoj Zsurnal (Élő Lap) volt: Hell áldozatává vált Borisz Akunyin író, Vlagyimir Pribilovszkij publicista, Viktor Alkszninsz, az állami duma képviselője és Valerija Novodvorszkaja politikus. Olykor a hekker a feltört accountokban kicserélte az avatárokat a Mihail Bojarszkij színész által alakított D'Artagnan muskétás fotójára, és így írta alá: „Önök mind pedofilok, én viszont – D'Artagnan vagyok."

* Az ebanyije_baranyi Alekszej Navalnij Twitter-oldala. – *A fordító megjegyzése.*



A feltört postafiókok tartalmát Hell a Virtuális inkvizíció című blogján publikálta.[136] Önmagát itt úgy jellemezte, mint „Jokert", aki „mindig és minden esetben száz százalékig eléri azt, amit akar", aki kész likvidálni bárkit, aki az útjában áll, meg úgy, mint aki „bármilyen létező módszert felhasznál arra, hogy irányítsa az embereket". A blogjában „olbanszkij"* nyelven írt, sajátságos módon elcsúfítva az orosz szavakat és folyamatosan káromkodva, posztjai legtöbbjét a „hehe" indulatszóval fejezte be.

Sokan meg voltak róla győződve, hogy Hell az elnöki adminisztrációtól kap pénzt vagy az FSZB-nél dolgozik: támadásai vakmerőek voltak és kizárólag ellenzékiek ellen irányultak. Miután feltörték a fiókját, Pribilovszkij Andrej Malgin újságíróval együtt indított nyomozást a Hell álnév alatt rejtőző ember felkutatása érdekében. A hekker nem egyszer tett róla említést, hogy az Orosz Bölcsészettudományi Egyetem (RGGU) történelem-levéltáros szakán tanult. Az önkéntes nyomozók beléptek az egyetem archívumába, és ott azoknak a hallgatóknak a személyes aktáját szálazták szét, akiknek az életrajza nagyjából illett Hell életének máshonnan ismert részleteihez. Kizárásos alapon Szergej Makszimovhoz jutottak el.

A fórumokon Hell néha a Szergej névvel lépett be, és Makszimként mutatkozott be. Kiderült, hogy évekkel ezelőtt Makszimov Németországba költözött – Navalnij blogját pedig éppen egy német IP-ről törték fel.[137] Pribilovszkij és Malgin létrehozta a Seryozha_vyhodi** blogot, ahol elkezdték részletesen felfedni a hekker valódi személyiségét. Hell a válaszában azt mondta, életrajza minden részletét menet közben gondolta ki, beleértve azt is, hogy az RGGU-n tanult.

Aktivisták fülese alapján, akik információkat kutattak

* Az olbanszkij az internetes mémek világában használt elferdített orosz nyelv, tele trágár kifejezésekkel. – *A fordító megjegyzése.*
** A blog neve magyarul: *Szerjózsa, kifelé!* – *A fordító megjegyzése.*

fel róla, Makszimovot a német rendőrök hamarosan letartóztatták oldalfeltörések és dokumentumhamisítás vádjával.[138] A bíróságon Makszimov azt mondta, hogy valóban Németországban él, és használta valamikor a Hell álnevet, de a hekkerrel csak leveleztek. A házkutatás során a számítógépén megtalálták Navalnij és felesége ezer levelét, blogjának screenshotjait, a jegyzetfüzetét az IP-címével, de egyébként Makszimovnál semmilyen hekkerprogram nem volt telepítve.

Az ügyészség két év börtönt kért Makszimovra, a bíró másfél évnyi feltételes szabadlábra helyezést és közmunkát szabott ki rá. Orosz hivatalos személyek nem keltek a védelmére. Hell hamarosan visszatért a blogja vezetéséhez: ahogy korábban, néhány hetente egyszer posztokat ír Navalnijról, amelyeket, úgy tűnik, senki nem olvas.

A korábbi feltörésekhez képest a Navalnij levelezésének kiszivárogtatása okozta következmények elég komolynak látszottak. A politikus úgy véli, a Kirovlesz büntetőügyet éppen a leveleinek publikálása után indították meg ellene. E levelek útján ezzel a társasággal bizonyos üzletek megkötéséről tárgyaltak. (Navalnijt és üzleti partnerét, Pjotr Oficerovot az állami vagyon eltulajdonításával vádolták.) Navalnij éppen a Kirovlesz-ügy kapcsán kihirdetett ítélet miatt nem indulhatott az elnökválasztáson (2018-ban).

*23. fejezet*

## A világításnak befellegzett

A háború Ukrajnában 2014 tavaszán kezdődött, mindössze néhány héttel az ország európai integrációját pártolók kormányellenes tiltakozásai után. A demonstrációk során tüzet nyitottak a tiltakozó tömegre, többen meghaltak, az országban forradalom zajlott le, Ukrajna elnöke Oroszországba menekült. Ezután a Donyec-medence városaiban az oroszbarát aktivisták és harcosok elfoglalták a kormányzati épületeket, az orosz csapatok inkognitóban megszállták a Krímet, és végül „hozzácsatolták" a félszigetet Oroszországhoz. Ezzel párhuzamosan az orosz csapatokkal kapcsolatban álló hekkerek elkezdték tesztelni Ukrajnában a kiberfegyverzetet.

2014 májusában, az elnökválasztás előestéjén a hekkerek megtámadták az ukrán központi választási bizottságot. A hekkerszervezet, amely magát Kiberberkutnak nevezte (és analitikusai kapcsolatban álltak az orosz titkosszolgálatokkal), blokkolta az ukrán belügyminisztérium és főügyészség, valamint az ukrán tévécsatornák weboldalait, továbbá ukrán politikusok postafiókjait törte fel. Az orosz hekkereket vádolták[139] annak a ballisztikus röppályák számítására szolgáló alkalmazásnak a feltörésével is, amelyet az ukrán tüzérség használt – ennek következtében a hadsereg a tarackjainak a nyolcvan százalékát elveszítette, és az emiatt bekövetkező tüzérségi hiba miatt halhattak meg többen, akik így közvetve váltak a hekkertámadások áldozataivá.

A legkomolyabb epizód a kiberháborúban 2015. december végén zajlott: nem sokkal az után, hogy egy kis időre áram nélkül maradt az Oroszországhoz csatolt Krím.

December 23-án napközben az ivano-frankivszki körzet energetikai alállomásait igazgató egyik központ operátora észlelte,[140] hogy a képernyője kurzora megrándult, pedig ő maga semmit sem csinált. A kurzor az egyik alállomás késes kapcsolóját működtető irányítógomb felé mozdult, és kikapcsolta azt. Az operátor megpróbált javítani a helyzeten, de a számítógép nem engedelmeskedett, aztán őt is kidobta az alállomás igazgatási rendszeréről. Hamarosan egész Ivano-Frankivszkban áramszünet állt be.

Ahogyan azt a Dragos Security társaság biztonsági szakembere, Robert Lee állítja, a hekkerek a feltörésre fél évig készültek. Először a számítógépekre telepítették a *Blackenergy 3* programot. Ennek érdekében a bevált módszert alkalmazták: a hálózat felhasználóinak adathalász leveleket küldtek Microsoft Word-fájlokkal, amelyek a makrók telepítését ajánlották fel. Ez pedig kártékony programot juttatott a gépre.

Az elosztócentrumok belső hálózatai a tűzfalak révén gondosan el voltak különítve az alállomásokat irányító centrumtól. A *Wired* című újság megjegyezte, hogy ez a védelem jobb, mint az amerikai elektromos hálózatot irányító társaságokéi. Ennek ellenére a hekkereknek sikerült feltörniük: megszerezték a fogyasztók adatait és a behatoláskor sikerült hétköznapi áramfogyasztóknak mutatni magukat.

Annak a tanulmányozására, hogy hogyan épül fel elosztóközpontok hálózata és hogyan kapcsolódik az alállomások irányítási rendszerével, a bűnözőknek rámenett néhány hónapjuk. Ez alatt az idő alatt új firmware-t írtak az alállomások áramátalakítói számára, amelyek a világhálón keresztül kapott jelet átadták a késes kapcsolóknak. Amint egy szakértő megjegyzi, ez volt az első olyan feltörés, ahol a hekkerek magát a berendezést tudták átprogramozni.

Miután megkezdték a támadást, a hekkerek három központi elosztóból kettőben, amelyeknek a hálózatához hozzá tudtak férni, kikapcsolták a folyamatos áramellátásért felelős forrásokat. Ezután gigantikus mennyiségű telefonhívást eresztettek rá a Prikarpatyeoblenergo vállalat ügyfélszolgálatára, hogy a lakosok ne tudjanak bejelentést tenni az áramszünetről. Ezzel egy időben kikapcsoltak harminc alállomást, a konverterek firmware-jeit pedig úgy programozták, hogy az operátorok nem láthattak rájuk a központból. A késes kapcsolót csak kézzel lehetett átállítani. A hekkerek olyan programot engedtek rá az operációs rendszerre, amely lehetetlenné tette az újraindítást.

A régióban csak hat órával később sikerült helyreállítani a világítást, és a késes kapcsoló online átállítását nem is sikerült megjavítani – az áramátállítókat újabbakkal kellett pótolniuk. Amint a *Wired* hangsúlyozza, az USA-ban egy ilyen támadás következményei rendkívül súlyosak lehetnének, mivel ott az alállomásokon a késes kapcsolót kézzel átkapcsolni nincs mód.

Az ukrán hatóságok a támadás mögött Oroszországot sejtették. A *Reuters* szintén rámutatott, hogy a BlackEnergy programot korábban az orosz hekkerek használták. Ezenkívül a BlackEnergy név ahhoz a hekkercsoporthoz tartozik, amely a Bad Rabbit és a Petya nevű, tömeges károkat okozó vírusokat fejlesztette ki: ezek a fertőzött számítógépeken rejtjelezték az adatokat, és váltságdíjat követeltek a felhasználóktól a blokád feloldásért. Így vagy úgy, de *Wired* által kérdezett szakemberek nem tudták egyértelműen megmondani, ki szervezte a támadást az Ivano-Frankovszkban. Nem lehet kizárni azt a verziót sem, mely szerint a hekkerek először az ukrán villamosenergia-központ számítógépes hálózatát törték fel, majd pedig e munkájuk eredményét eladták Oroszországnak.

* * *

2016. február 6-án a Conflict Intelligence Team kutatócsoport munkatársa, Ruszlán Levijev késő éjszakába nyúlóan a számítógépe előtt ült. Reggel kívánta közzétenni várhatóan nagy port kavaró anyagát. Ez a 6-os számú, Nyizsnyij Novgorodnál állomásozó orosz tankcsapat részvéte-

lét ecsetelte[141] az Ilovajszk és Debalcevo alatti csatákban a Donyec-medencében. Az egyik bizonyíték az orosz csapatok részvételére az ukrán konfliktusban egy Levijev által készített fotó volt, amelyen Szergej Sojgu védelmi miniszter karórával tünteti ki az egyik sebesült katonát a moszkvai Burdenko klinikán. Levijev a Twitteren tette közzé a képet.

Nem ez volt az első alkalom, hogy a katonáik donyecmedencei részvételét tagadó orosz hatóságokat komoly vádakkal illető dokumentumot publikált. Levijev mégis viszonylagos biztonságban érezte magát Moszkva déli részén lévő lakásában, bár nemegyszer kapott fenyegetést, az utcán pedig észrevette, hogy követik.

Az utóbbi években Levijev együttműködött a Bellingcat nevű csoporttal. A team nyilvános forrásokon, mint például közösségi oldalakon közölt fotókat használt fel, és vizsgálta az orosz katonák részvételét az ukrajnai és a szíriai konfliktusokban. A holland hatóságok a Bellingcat adatait használták fel[142] a maláj Boeing-gép szerencsétlenségének kivizsgálásakor is, amelyet Donyecktől nem messze lőttek le 2014 júniusában. 2018-ban épp a Bellingcat tudta bizonyítani, hogy az Oroszországban hazaárulásért elítélt Szergej Szkripal és lánya megmérgezésével vádolt Ruszlan Bosirov és Alekszandr Petrov álnéven működő GRU-ügynökök voltak.

Mivel elképzelhető volt, hogy nagyobb figyelem irányul majd rá, Levijev arra az esetre, ha kiszállnának hozzá a bűnüldöző szervek és lekapcsolnák az áramot, a lakásában négy tartalék akkumulátort üzemelt be, és Yota mobilinternettel kettőzte meg a hálózati csatlakozását.

Éjjel három óra körül Levijev átnézte a szövegét, a tördelést is ellenőrizte. Mellette aludt két macskája, Kotopusz és Deszantnyik. Ebben a pillanatban a mobiltelefon képernyője, amely Levijev mellett az asztalon hevert, villogni kezdett.

Levijev látta, hogy gyors egymásután értesítések érkeztek a Twitteren, majd egy perc múlva még kettő a Facebookon. Mindegyik a fiókjai feltörésének kísérletéről szólt.



Levijev azonnal megváltoztatta a jelszavait a közösségi oldalakon, és ellenőrizni kezdte a többi accountját. A messengereivel és a munkahelyi postájával semmi nem történt, de a hekkereknek sikerült feltörniük Levijev Yandexen lévő fiókját – bár azt, hogy ez hogyan történt, a mai napig nem érti, hiszen azt kétlépcsős hitelesítési védelemmel látta el, amely a mobiltelefonjához volt kapcsolva.

A feltört e-mailek segítségével a hekkerek visszaállították Levijev Zsivoj Zsurnal-belépését, és az itteni accountján keresztül beléptek a Bellingcat adminisztrációs paneljébe. Levijev Bellingcaten található oldalán a következőt posztolták: „A Bellingcat a provokátorok NATO- és Amerika-barát szervezete, hazudnak és kémkednek, mások problémái számukra a megélhetést jelentik. Szemétládák, nem pedig kutatók."

A feltörésért a Kiberberkut vállalta magára a felelősséget.[143] A hekkerek megszerezték a hozzáférést Levijev iCloudjához is – a kutató ide feltöltött személyes fotóit, útlevélmásolatát és lakcímét később kitették a Kiberberkut weboldalára.

Az amerikai ThreatConnect társaság, amely a kiberbűntények felkutatásával foglalkozik, részletesen megvizsgálta[144] a Levijev és a Bellingcat elleni támadást. A hozzájuk rendszeresen érkező adathalász levelek úgy néztek ki, mint a Google értesítései arról, hogy az account egy illetéktelen behatoló áldozatává válik. A levélben levő hivatkozások phishing weboldalakra mutattak. A domaineket, amelyeket a ThreatConnect adatai szerint a támadáshoz használtak fel, a német hírszerzés és az elemzést végző társaságok a Fancy Bear csoporthoz köthetőnek nevezték,[145] akik körülbelül ugyanebben az időben az amerikai Demokrata Párt szerverét törték fel. „Az alapján, ahogyan működnek, és ahogyan az infrastruktúrát használják, rá lehet jönni, hogy a Kiberberkut és a Fancy Bear vagy ugyanaz a csoport, vagy harcostársak, akik együttműködnek" – mondta nekem a ThreatConnect vezető elemzője, Rich Barger.

*24. fejezet*

## Feltörők állami szolgálatban

Az orosz nyelvű hekkerek között érvényben van néhány titkos szabály. Ezek közül az egyikről, a „Ne dolgozz a .ru területén"-ről már beszéltem. Léteznek más, nem titkos szabályok is: ha a feltörés során találsz valamit, ami érdekelheti a „rezsimet", akkor oszd meg vele, illetve amikor segítséget kérnek tőled hazafias ügyekben, működj együtt. E hallgatólagos szabályok elutasítása bűncselekménnyel ér fel.

2001 elején az az UFO nevű hekker, akit lefüleltek a titkosszolgálatok, elmondta,[146] hogy miután beszélt a nyomozókkal, felajánlották neki, hogy találkozhat az egyik olyan szervezet szakértőjével, amelyik közel áll a titkosszolgálatokhoz. Az illetőt Szidorovnak hívták. A hekker a letartóztatása után néhány hónappal hazamehetett, és az anyja azt mondta, telefonon kereste egy ismeretlen férfi, és meghagyta a telefonszámát. A hekker visszahívta a férfit. Szidorov volt az, aki közölte, hogy látta az ügyéről szóló szakvéleményt, és érdeklődik a tevékenysége iránt.

Hamarosan egy moszkvai étteremben találkoztak. Szidorov azt mondta, szüksége van egy munkatársra, hogy ahogy UFO teszi, a sebezhető pontok felkutatásával foglalkozhasson. A férfi jó fizetést ígért, és a hekker beleegyezett az együttműködésbe. Az épület, ahol dolgoznia kellett, „igencsak felszereltnek" látszott. Hamarosan megjelent a vezetés is: megkérdezték UFO-t, hogyan tudja kikerülni a tűzfalak különböző típusait, hogyan tör fel idegen IP-ket,*

* Lásd *Fogalomtár.*



és hogyan juttatja a távoli rendszereket „a szolgáltatások megtagadása" állapotba. A hekker átment a teszten. A következő néhány hónapon keresztül sikeresen abszolvált még néhányat, és meg is kezdték az állományba vételét, de váratlanul új vezetés érkezett, amely úgy döntött, hogy nem vesz fel önkénteseket.

Az FSZB CIB – a titkosszolgálatok főhivatala, amely kapcsolatban áll a hekkertevékenységgel – egy munkatársa azt nyilatkozta a *Hekker*nek, hogy a kollégák „meggyőződésből" érkeznek hozzájuk. „Az FSZB alapvetően abban különbözik bármelyik kereskedelmi cégtől, hogy a szakemberek nálunk nem dolgoznak, hanem *szolgálnak*, és ez nagyon fontos momentum – mondta. – A minden más egyébre vonatkozó egyenlő feltételek mellett az a pénzösszeg, amit nálunk és amit az üzleti szférában valaki meg tud keresni, nagyban különbözik. A munka az FSZB-nél nem holmi amerikai bestseller a megfoghatatlan »Bondok« életéből, a mi munkánkban egy csomó rutin van, bár akad, aki egészen regényes momentumokat is talál benne."

Anton (kérésére a nevét megváltoztattuk), aki főállásban vírusanalízissel foglalkozik, időnként érintkezésbe lép az FSZB munkatársaival. Szavai szerint a CIB-ben kevés a műszaki munkatárs, ezért gyakran vonnak be külső szakembereket. „Létezik az illegális hekkerek bevonására, ösztönzésére, munkalehetőségeik megteremtésére egy széles körben elterjedt séma, hogy rajtuk keresztül megkapják a szükséges információkat" – magyarázza a hekker. Ahogy ő fogalmazott, a hekkereket gyakran elhelyezik akár védett lakásokban is, hogy ne tudja őket elkapni a rendőrség. Anton tud néhány olyan esetről, amikor a Belügyminisztérium „K" ügyosztályának embereit letartóztatták ugyan, de aztán a letartóztatottakért megérkeztek az FSZB munkatársai, és a következő szavak kíséretében vitték el őket onnan: „Nem a maguk dolga."

Néhányan a hekkerek közül a bűnüldöző szervekhez mentek át főállásba. A *The New York Times* forrásai[147] meg-

erősítik, hogy az orosz hekker, Jevgenyij Bogacsev, akit évekig kerestek az amerikaiak, a titkosszolgálatokkal dolgozik együtt. Bogacsev hozta létre a fertőzött számítógépek hálózatát világszerte (Oroszországot kivéve), amivel százmillió dollárt keresett, később bankokat, massachusettsi rendőrségi ügyosztályokat és olyan észak-karolinai cégeket támadott meg, amelyek programhiba-kereséssel foglalkoztak. A *The New York Times*-os forrásom szerint, amíg Bogacsev lopta a pénzt, az „orosz hatóságok elnéztek a feje fölött", miközben ugyanazokkal a számítógépekkel dolgoztak a fájlok és az elektronikus levelek felkutatásán: állítólag a fertőzött amerikai számítógépeken lévő, az ukrajnai és szíriai konfliktusra vonatkozó titkosított információk érdekelték őket, de a keresést a „teljesen titkos" és a „védelmi minisztérium" kulcsszavak mentén végezték.

„Azt beszélik, hogy [Bogacsev] gondtalanul él Anapában, és segít az FSZB-seknek – mondja a hírforrásom, aki kibertámadás-elemzéssel foglalkozik. – Miért is ne? Hogyha FSZB-s lennék, természetesen megfejném. Oroszországban él, van egy rakás hozzáférése, vétek lenne ezt nem kihasználni, miközben azt se szabad elfelejteni, hogy ő bűnöző."

2012 tavaszán Anton megkapta újabb feladatát: törje fel az egyik vezető orosz hírügynökség honlapját. A megbízók kérték, hogy igyekezzen: attól féltek, hogy Vlagyimir Putyin elnöki beiktatása előtt a bűnözők valami nem kívánatos dolgot fognak közzétenni Vlagyimir Vlagyimirovicsról a weboldalon. Anton könnyedén teljesítette a megbízást, ahogy ő fogalmazott, a hírügynökségnél semmiféle védelem nem létezett a támadás ellen: „Csak egy csomó régi kód volt, amiket még a 2000-es évek elején írtak." Mint általában, jelentést írt a feltörésről és átadta a vezetésnek. Egy év múlva a hekker, mivel érdekelte a dolog, úgy döntött, ellenőrzi, hogy a hírügynökség hogyan védekezett a



távolról jövő feltörések ellen. Az összes általa fellelt védelmi rés fennmaradt.

Egy hekker, aki a titkosszolgálatoknak, többnyire az FSZB-nek dolgozott, azt mesélte, hogy amint valakit felbéreltek a hekkerek közül, rajta keresztül próbálták az ismerőseit is beszervezni és csapdába csalni. Az FBI kibervédelmi osztályának korábbi különleges ügynöke, Milan Patel elmondta,[148] hogy az Egyesült Államok és Oroszország sokáig együtt hajtott végre műveleteket a hekkerek elfogására, de aztán a helyzet megváltozott: „Egy konkrét emberrel kapcsolatban, akit kerestünk, tájékoztattuk őket, de az illető titokzatos módon eltűnt, hogy azután már az orosz kormány szolgálatában jelenjen meg. Lényegében azzal, hogy közöltük az FSZB-vel, kire vadászunk, segítettünk nekik összeszedni a tehetséges hekkereket."

Az orosz titkosszolgálatok nyilvánvalóan máig folytatják a hekkerek verbuválását a büntetőügyük lezárásáért cserébe. 2018 júliusában Belgorodban a bíróság megszüntette[149] a büntetőeljárást egy helyi lakossal szemben, aki ötszáznegyvenöt kibertámadást hajtott végre az FSZB hivatalos weboldalai ellen. Az ügyet az FSZB vizsgálatot végző munkatársainak közbenjárására állították le.

Az FSZB-nél hírforrásokat találni szinte lehetetlen. A sajtónak soha nem nyilatkoznak, a közvélemény számára ismert, azaz a nem fedett munkatársaik sem válaszolnak a megkeresésekre, és általában csak zárt rendezvényeken vállalnak fellépést.

Egy ideig kétségbe voltam esve emiatt, de pontosan tudtam, hogy a riporterek az idejük kilencven százalékát vagy azzal töltik, hogy várnak az információkra, vagy azzal, hogy megpróbálják azokat megszerezni. A soron következő nagy kiberkonferencián, amelyet Moszkvában rendeztek, megkérdeztem a szervezőktől, hogyan találhatnám meg az ideérkezők között a titkosszolgálatok munkatársait. Az egyik szervező ezt mondta: „Ők azok, akik név-

tábla nélkül mászkálnak." A következő szünetben kimentem az előcsarnokba, és miközben a tartaletkákkal* dúsan megrakott asztalok között járkáltam, névtábla nélküli embereket kerestem. Végül hármat találtam, de csak az egyik egyezett bele a beszélgetésbe.

Ő megerősítette, hogy a hekkereket fel szokták kérni konzultációra a titkosszolgálatok. Ahogy ő fogalmazott, a más országokat érintő kibertámadások nem az FSZB illetékességébe tartoznak: „Ezekkel az ügyekkel régóta és sikeresen a GRU-ba felvett önkéntesek és kibercsapatok foglalkoznak."

* A tartaletka édes vagy sós töltelékkel töltött, tésztából készült kis kosárka alakú étel. – *A fordító megjegyzése.*

*25. fejezet*

## Geraszimov doktrínája

A 2010-es évek eleje vízválasztó az orosz hekkerek és az állami kiberháborúk történetében. Addig a hatóságok megbízásait egyes bűnöző hekkerek vagy aktivisták teljesítették, ettől kezdve viszont az állam összeállított egy állandó kibercsapatot a katonai részlegei számára.

Az első meghatározó dokumentum[150] a kiberháborúról a 2011-es év végén jelent meg, amikor a védelmi minisztérium kibocsátotta *Az Oroszországi Föderáció haderejének koncepciója az információs térben folytatott tevékenységről* című jelentését. Eszerint a hivatal nem szándékozik beleavatkozni más országok belügyeibe, de támogatni fogja a tulajdonképpeni kiberháborúkat a biztonság érdekében, és „kész a katonapolitikai jellegű fenyegetéseket visszaverni az információs térben". A védelmi minisztérium konfliktus esetén vindikálja magának „a jogot az individuális vagy a kollektív önvédelemre, bármilyen módszer és eszköz felhasználásával".

Két évvel később a GRU egyik kurátora, Valerij Geraszimov tábornok a *Voenno-promislennij Kurjer* (Hadiipari Kurír) című lapban publikálta[151] azt a szöveget, amelyet később Geraszimov-doktrínának neveztek el. A cikkben hibrid háborúról írt, amely alkalmazza a kiberháborút is, például a robbantásos tevékenységek esetén abból a célból, hogy az intervenció előtt előkészítse a hadszínteret.

Az új doktrína ténylegesen megújította az orosz felderítőhagyományt. Az ezt megelőző időszakban a GRU mindenekelőtt saját ügynökeinek a megfelelő szervezetekbe való beépítésével, valamint a stratégiailag fontos intézményei

számára hivatalnokok és munkatársak verbuválásával foglalkozott. Még egy fontos iránya volt a hivatal tevékenységének: a dezinformálás. Jóval a *fake news* terminus megjelenése előtt a KGB felderítői és a munkatársai azt a fals információt terjesztették, hogy az Egyesült Államok az 1950-es években Koreában biológiai fegyvereket vetett be, illetve azt, hogy az amerikai titkosszolgálatok rendelték meg John Kennedy meggyilkolását.

A hadviselés új, hibrid módszereinek legfontosabb elemei a hekkerek és a kiberharcosok lettek. Ezek között ott vannak azoknak az utódai is, akik egykor dezinformációt terjesztettek: most ők azok a „trollgyári munkások", akik az orosz hatóságokkal kapcsolatban állva igyekeznek Facebook-posztokkal és -kommentekkel megosztani az amerikai társadalmat (egészen a *Csillagok háborújá*ról szóló negatív vélemények közléséig).[152]

A legismertebb „gyár" Jevgenyij Prigozsin nevéhez kötődött. A milliárdost Vlagyimir Putyin jó ismerősének tartják (Prigozsin cége az évek során sokmilliárdos állami cateringszerződéseket nyert el, beleértve a Kreml vendégeinek kiszolgálását is). Az első „gyár" székhelye eleinte a szentpétervári Olgino-negyedben volt (emiatt kezdték „olginói botnak" nevezni), aztán Szentpéterváron, a Szavuskin utcában, ahol „Internetkutató Ügynökségnek" hívták. Tucatnyi munkatársa nap mint nap azért járt dolgozni ebbe az épületbe, hogy álhíreket találjon ki, és megírja (kitalált néven) a kommentjeit az orosz és a külföldi közösségi hálókra és fórumokra, dicsőítve vagy szidva bizonyos politikusokat.

A gyár egyik munkatársa azt mesélte,[153] hogy a műszak akár tizenkét órán át is tarthat. Mindenekelőtt megkapja az instrukciókat – például, hogy sértő kommenteket írjon Petro Porosenko ukrán elnökről, vagy írja azt, hogy az orosz ellenzék készítette elő Borisz Nyemcov meggyilkolását.

2016-ban a trollkodó aktivisták számára a fő téma ismét az Egyesült Államok lett: közeledett az elnökválasztás,



és a gyár munkatársai a Facebookon több száz csoportot és accountot létesítettek, hogy így vagy úgy, de Donald Trump jelölését támogassák, és agitáljanak Hillary Clinton ellen. Az egyik posztban például ezt közölték:[154] „Ma Amerika elnököt választ az istenfélő erkölcsi elvek alapján. Hillary maga a sátán, hazugságai és bűnei mutatják, milyen gonosz. Még ha Donald Trump se egy szent, végtére is tisztességes ember, mélyen átérzi ezt az országot. Én neki adom a szavazatomat!"

A gyár munkatársai amerikaiaknak tettették magukat, még gyűléseket is szerveztek a jelölteket pártolóknak és azokat ellenzőknek az Egyesült Államokban. Hogy mindez mennyire befolyásolta a választások eredményét, amit végül is Trump nyert meg, hitelt érdemlően lehetetlen megmondani. 2018 februárjában az amerikai hatóságok keresetet indítottak az Internetkutató Ügynökség tizenhárom munkatársa ellen azzal a váddal, hogy beleavatkoztak az amerikai választásokba: az amerikai igazságügyi minisztérium azt emelte ki, az oroszok célja az volt, hogy „viszályt szítsanak a társadalomban".

2018 novemberében amerikai kibercsapatok sikeres[155] támadást hajtottak végre az Internetkutató Ügynökség ellen. Az USA kongresszusi választásának napján az USA-nak sikerült kikapcsolnia az internetet a „trollgyár" irodájában, hogy ezzel megzavarják a szavazás befolyásolását célzó tevékenységét.

* * *

A „tudományos századok" ötletét – amelyeknek az orosz kiberhadsereg alapjává kellett válniuk – a hadsereg vezetői kezdeményezték 2013-ban.

Nem sokkal korábban lett védelmi miniszter Szergej Sojgu. Kinevezése után azonnal érdeklődést mutatott a kibervédelem iránt, és nyilatkozatot tett az orosz kiberhadseregek felállításának szükségességéről – párhuzamosan az amerikai Cyber Commandokkal, amelyek az USA védelmi minisztériumának alárendelve működnek, és háborús ki-

berműveletekkel, valamint az amerikai számítógép-hálózatok védelmével foglalkoznak. 2013 júliusában Sojgu nyilatkozatot tett a fiatal programozókat célzó „nagy vadászat" kezdetéről. „A vadászat itt a szó jó értelmében szerepel, ezt annak a hatalmas programozási tevékenységnek az igénye diktálja, amely a hadsereg számára szükséges az elkövetkező öt évben" – jelentette ki[156] az informatikai védelmet oktató műszaki főiskolák rektorai előtt.

Hogy mennyire konkrét dolgokra fogják használni a matematikusokat és a programozókat, arról Dmitrij Rogozin miniszterelnök-helyettes nyilatkozott, aki a védelmi szerveket felügyelte. Az orosz hivatalnokok közül először ő nyilatkozott a kiberhadseregek létrehozásáról. „Ez az állami infrastruktúra informatikai védelmének biztosításával függ össze" – közölte[157] Rogozin. A hírforrások rámutattak,[158] hogy az orosz kiberhadsereg alapvető feladatává egyfelől az „olyan információk feldolgozása válik, amelyek kívülről érkeznek, másfelől pedig a kiberfenyegetések elleni küzdelem": minden szolgálattevőnek nyelvi előkészítőn kell átmennie, és meg kell tanulnia angolul.

Sojgu szándékainak komolyságát a *Vesztyi Nyegyeli* (A hét hírei) című tévéműsorban is megerősítette egy évvel a kinevezése után, 2013 októberében, amikor az Oroszországot érintő új fenyegetésekről beszélt. Az egyik ilyen fenyegetésként a kiberfegyvert nevezte meg. „Ez, természetesen, egyre közelebb és közelebb kerül a »tömegpusztító fegyver« fogalmához – fejtegette a védelmi miniszter. – Egészen közel kerültünk ehhez, és azt mutatja a különböző országok hekkereinek tevékenysége is, hogy ennek révén mindent el lehet érni, amit csak akarnak." Sojgu lényegében Vlagyimir Putyinnak az „informatikai támadás megsemmisítő erejéről" szóló szavait ismételte meg,[159] amelyek az elnök három hónappal korábbi, az orosz biztonsági tanácsban tett felszólalásában hangzottak el.

2014 tavaszán a védelmi minisztériumban megjelentek[160] az „információs műveletek csapatai" a potenciális ellenséggel folytatott kibernetikai ellenállás érdekében. Később a védelmi minisztérium forrásai kifejtették,[161] hogy ezeket „a potenciális ellenség információs hálózati munkájának megzavarására" hozták létre.



A „tudományos századok" alakulatai országszerte létrejöttek a hadseregben. Ide kezdték összegyűjteni a műszaki főiskolán végzetteket: matematikusokat, programozókat, kriptográfusokat, mérnököket. A jelentkezési űrlapon[162] meg kellett jelölni a programozási nyelvek és a szoftverek ismeretét. A Novoszibirszki Állami Egyetem a hallgatók között meghirdette a toborzást[163] Oroszország védelmi minisztérium szergijev-poszadi központi kutatóintézetének tudományos századába, hogy „részt vegyenek a szuperszámítógépes technológiák alkalmazásában". 2015 szeptemberében a védelmi minisztérium irányítása alatt megnyílt az IT-technológiák kadétiskolája,[164] három hónappal később pedig a Katonai Híradó Akadémián már végeztek is[165] az információbiztonság tudományos századának első végzős növendékei.[166]

A hallgatók mellett a védelmi minisztérium igyekezett behívni[167] „olyan hekkereket is, akiknek problémáik vannak a törvénnyel". Ezt az információt a kiberkutató társaság, a CrowdStrike (ez részben azokat a feltöréseket vizsgálta, amelyeket a Fancy Bear hajtott végre) egyik vezetője, Dmitrij Alperovics megerősítette:[168] „Amikor olyasvalaki kerül a látókörünkbe az orosz kiberalvilágból, aki műszaki tudással van felvértezve, büntetőügy indul ellene, de aztán nyom nélkül eltűnik" – magyarázta.

* * *

2015 júliusában a VKontaktén megjelent egy videó, amely jelentkezésre buzdított a kiberhadseregbe. A videón egy férfi újratölti az automata fegyverét, majd leteszi az asztalra a notebookja mellé. Aztán elkezdi beütni a klaviatúrán a programkódot. Kemény rock szól a háttérben, a kép felső részén pedig megjelenik egy felirat: „Az Oroszországi Fö-

deráció tudományos százada". A videón, amely a hekkerekről szóló filmek szellemében született, a következő szlogen villog: *Ha sikeresen elvégezted az egyetemet, ha a műszaki tudományok szakembere vagy, és készen állsz alkalmazni ismereteidet – mi megadjuk neked a lehetőséget!* Az érdeklődőknek „nagy kapacitású számítástechnikai komplexumokban folytatott munkát" ígérnek. A film anyagául részben egy vírusvideó[169] kockái szolgáltak *Én egy orosz megszálló vagyok* címmel, amelynek hőse szarkasztikusan „bocsánatot kér" a nézőktől Szibéria, a Baltikum, Közép-Ázsia és Ukrajna elfoglalásáért. „Jól figyeljenek: nekem nem kell a maguk képmutató »szabadsága«, nekem nem kell a maguk rothadó »demokráciája«, tőlem idegen mindaz, amit önök nyugati értékeknek neveznek. Szívesen figyelmeztetem önöket most, utoljára: ne botoljanak belém! Én teszek a békéért, én szeretem a békét, de harcolni mindenki másnál jobban tudok."

A tudományos századokba hívó agitációs videót kitették a Tambov városához tartozó katonai oktatási központ honlapjára is, itt szintén létrehoztak egy ilyen századot. Ugyanez a videó jelent meg a naucsnajarota.rf weboldalon is. A már-már karikaturisztikus módon ábrázolt kiberkatona képe némiképp hasonlított a Fancy Bear[170] weboldal videójára: ez ahhoz a hekkercsoporthoz tartozik, amelyet Oroszország érdekében végrehajtott nemzetközi feltörésekkel vádoltak.

A tambovi oktatási centrum egyik tanára, Anatolij Baljukov kifejtette,[171] hogy „növendékeink fő feladata a (kibertámadás) módszereinek elsajátítása, és egy reménybeli védőcsapat felállítása. Emellett a hallgatóknak ki kell dolgozniuk a kibertámadás algoritmusait, hogy bármilyen esetben maximális hatékonysággal tudják azokat használni". A dokumentumokban, amelyeket kiposztoltak az oktatási központ közössége számára, azt állították, hogy az alosztályok „a hálózatok támadhatóságát, a programbiztonságot kutatják".

A vezérkarnak van tudományos százada a krasznodari



körzetben is.[172] A védelmi minisztérium weboldalán található információ szerint ebben a körzetben folyamatosan két szakasz tartózkodik, egyenként harminc emberrel. Napirendjük[173] nem sokban különbözik a hadseregétől: hatkor van az ébresztő (kivéve vasárnap, amikor hétkor), aztán ötven perc torna, reggeli, kilenc óra után pedig a „tudományos munka" következik.

Aki be kívánt lépni a századba, annak ki kellett töltenie egy űrlapot, ahol a titkosításra vonatkozó és matematikai kérdések mellett a szüleiről is kérdezték, és arról, szeretne-e valami újat létrehozni a védelmi minisztérium számára, valamint arról, hogyan viszonyul az államtitkokhoz való hozzáféréshez. A szerződés megkötése után tiszti rangot és harmincnyolcezer rubel fizetést ígértek. A brosúrában, amely a tudományos században végzett munkát reklámozza, lehet találni egy „teaszobáról", illetve „a pszichés tehermentesítés szobájáról" készült fotót is. Ezeket a helyiségeket a kiberhadsereg számára létesített kaszárnyában alakították ki. Az egyik szobában van egy asztal teáskannákkal, a falakon tájképek függenek, a másik pedig olyan, mint egy vendégszoba, két dívánnyal és egy akváriummal.

Válaszul a kérésemre, amely egy tudományos század meglátogatására és a védelmi minisztérium katonai megbízottjával készítendő interjúra vonatkozott, felhívtak, és közölték, hogy a hivatalt senkinek sem mutatják meg, arról senkinek nem beszélhetnek, „azért, hogy senki ne tudhassa meg, hogyan alkalmazzuk ezeket a századokat". „Ezt a témát lezárták az olyan szövetségi szervezetek, mint például amelyiknek a nevében *o* betű szerepel,* és az FSZB – tette hozzá a hivatal képviselője. – A továbbiakban ne kockáztasson azzal, hogy a látóterünkbe kerül".

A védelmi minisztérium soha nem beszélt nyíltan a kiberháborúk megszervezéséről, azok méretéről és mun-

* Itt a minisztérium képviselője valószínűleg az FSZO-ra, a Szövetségi Biztonsági Szolgálatra utalt. – *A fordító megjegyzése.*

katársainak létszámáról. Egyébként a minisztériumhoz közeli kiadványokban és magának az intézménynek a weboldalán időnként megjelennek anyagok az elért eredményeikről.

Például 2014 szeptemberében a védelmi miniszter helyettese, Jurij Szadovenko arról beszélt[174] a rjazanyi légidesszant-főiskolán zajló találkozón, hogy „megkezdték a kibervédelem kérdéseinek elsajátítását". A védelmi minisztérium azt közölte,[175] hogy a 2015 szeptemberében tartott *Sit-Szojuz-2015* hadgyakorlat során az orosz haderő a kibertámadások visszaverését is szimulálta, felderítésére képes tűzfalakat és más védelmi programokat telepítettek, amelyek kiszűrték a számítógépek felé irányuló gyanús hálózati csomagokat.

A tudományos századok előmozdítása érdekében a Zvezda tévécsatorna 2014-ben egy negyvenrészes tévésorozatot[176] sugárzott *Botok* címmel azokról az újoncokról, akik bekerültek a kiberhadseregbe. A filmsorozatban a védelmi minisztérium vezérkari főnöke az egyik harci egység vezetőjét azzal bízza meg, hogy hozzon létre egy alosztályt, amely a kiberfegyverkezéssel foglalkozik. A sorozatban a következő vicces mondat hangzik el: „minden csatlakozónak egyórányi internethasználat jár". A Zvezda tévécsatorna a sorozatot így reklámozta: „A felvételek befejezésének idejére ismertté vált, hogy az orosz védelmi minisztériumban elhatározták: az orosz hadrendszer és a vele kapcsolatos hivatalok különböző jellegű kibertámadásoktól való védelmével a speciálisan erre létrehozott informatikai műveleti hadseregek foglalkoznak majd."

Az *Armija Szegondnya* (A Hadsereg Ma) címet viselő kiadvány, amely a védelmi minisztérium tevékenységét világítja meg, összehasonlította[177] a tudományos századok munkáját a *James Bond*-filmekkel: „A legújabb filmben a számítógép-specialista, Q átnyújt az ügynöknek egy kis bőröndöt, és ezt mondja: »Több kellemetlenséget tudok okozni önnek pizsamában a laptopom előtt, mint amit maga végez egy év alatt a műveleti tevékenységével.« Íme, ilyen szakembereket akarnak kiképezni az orosz kiberhadseregekben."

„Szinte biztos, hogy 2014-ig Oroszország – eléggé naivan – nem foglalkozott saját jelenlétével a kibertérben – jelentette ki a Kaspersky Lab vezető biztonsági szakértője, Alekszandr Gosztyev. – Az ilyen munkához szakemberekre van szükségük – emiatt választották a »tudományos századok« formát."

Gosztyev mutatott nekem egy fényképet, amelyen a védelmi minisztérium reklámkiadványának oldalai látszottak. Ebben *Az Oroszországi Föderáció fegyveres erőinek vezérkara főhivatalának tudományos századaiba tartozó operátorok tudományos tevékenységének alapvető irányvonalai* címmel publikáltak számítógépek előtt ülő katonákról fotókat, demonstrálva, hogy a feladatuk nem más, mint a „védelem speciális programjának a kidolgozása".

Körülbelül 2014 elejére a védelmi minisztérium kötelékében létrehozták a Speciális Fejlesztési Központot. Ennek a munkatársai kezdtek el keresgélni álláskereső portálokon a műszaki egyetemek végzősei között. Mindenekelőtt az exploitokhoz és a kódvisszafejtéshez volt szükségük emberekre.

Az álláskereső portálokon jelezték, hogy a központ olyan munkatársakat keres, akik „kiváló ismeretekkel rendelkeznek a különféle szoftvertermékek forráskódjainak elemzése terén az IB [informatikai biztonság] területén végzett érdekes munka számára". A munkatársak N3-as besorolást kaptak (azaz bejelentési kötelezettséggel tartoznak külföldi út esetén), és százhúszezer rubelt elérő fizetést. A hirdetményben az is szerepelt, hogy az iroda csendes környéken található: egy folyó mellett Moszkva északi részén.

Ahogyan egy orosz informatikai védelmi cégnél dolgozó hírforrásom közölte, kereskedelmi cégektől országos szinten körülbelül száz ember ment át dolgozni az orosz kiberhadseregekbe.

*26. fejezet*

## A reakciósok tudománya

Oroszországban tucatnyi olyan állami tudományos kutatóintézet létezik, amely a védelmi minisztériummal áll kapcsolatban. Ezek általában jelentéktelen, szürke, konstruktivista épületekben működnek, messze a gyalogos útvonalaktól. A hidegháború alatt ezeken a helyeken szakemberek ezrei dolgozták ki a biológiai és kémiai fegyvereket – de nem csak ezeket. Ugyanitt születtek meg – háborús célokra – az új technológiák alkalmazásának elvei és módszerei, amelyek tíz évvel később a kiberkonfliktusokban köszöntek vissza.

Az 1950-es évek közepén szovjet mérnökök kis csoportját teljesen lázba hozta Anatolij Kitov *Elektronnije cifrovije masini* (Elektronikus számítógépek) című könyvének megjelenése. Ez volt az első orosz nyelvű könyv a programozásról, amely részletesen magyarázta a számítógép belső rendszerét és azt, hogy ezeket a gépeket hogyan lehet használni a gazdasági életben, hosszú távon pedig akár a mesterséges intelligencia létrehozására. Kitov, aki ekkor még nem volt negyvenéves, azonnal a kibernetika vezető szovjet szószólója lett.

Szamarában született[178] 1920-ban egy Fehérgárda-tiszt és egy cukrászdai alkalmazott családjában. Hogy kevésbé szúrjanak szemet a bolsevikoknak, Kitovék 1921-ben átköltöztek Taskentbe, ennek köszönhetően nem érintette őket a Volga-menti éhínség, amelynek több mint ötmillió ember esett áldozatául. Útjuk nem volt egyszerű: Oroszországban tombolt a tífusz, volt, hogy a halottak az utcán hevertek ott, ahol Kitovéknak nem ritkán a szabad ég alatt kellett



éjszakázniuk. Kamaszként Kitov a repülőgépmodellek, a sakk és a matematika iránt lelkesedett.

Ötödik osztályban irodalomórán Kitov írt egy dolgozatot, amelynek a *Rózsaszín mese* címet adta. Ebben egy kisfiú írta le saját álmát: Taskentben, a központi piacon az üres polcokat kalácsok, pulykák, különféle sajtok, kolbászok, ruhák és cipők töltötték meg. Az ötödikes fiúhoz nem sokkal ezután megérkezett az NKVD* két munkatársa, és megkérdezték, kinek a felszólítására írt ilyen gúnyos szöveget, de eredménytelenül távoztak.

Középiskola után Kitov a Taskenti Egyetem matematika-fizika szakára jelentkezett, magfizikával akart foglalkozni. Két hónappal később kivitték a frontra, zajlott a nagy honvédő háború. A lövészárkokban is matematikát tanult, és átvette az első két évfolyam anyagát. A Kitov család archívuma őrzi az egyetemi matematikai előadásvázlatát 1944-ből, abból az időből, amikor Kitov osztaga élet-halál küzdelmet vívott az ukrajnai Szambor felszabadításáért.

A frontról visszatérve Kitov Moszkvába költözött, hogy a Dzerzsinszkij Tüzérségi Hadmérnöki Akadémia ballisztikai karán tanuljon. Ugyanott kezdett el tudományos referensként dolgozni, miután befejezte tanulmányait. Szergej Koroljov felajánlotta neki, hogy menjen át az ő rakétatervezői irodájára, de Kitov ekkoriban értesült az első elektronikus számítógépek megjelenéséről, és megállapodott az akadémia vezetésével abban, hogy a védelmi minisztérium megbízottjaként a 254-es speciális konstruktőrirodába (SZKB-254) kerül, ahol megszerezhette a hozzáférést a titkos dokumentumokhoz.

A különleges raktárban Kitov rábukkant az amerikai matematikus, Norbert Wiener *Cybernetics* (Kibernetika) című könyvére, amelynek alapján írt egy cikket az új tudomány-

* NKVD = Belügyi Népbiztosság, rövidítve NKVD, az államigazgatás belügyi ágának legfőbb szerve a Szovjetunióban 1934 és 1946 között. – A szerk.

ról és megpróbálta azt publikálni. Ez nem volt egyszerű, ugyanis 1952-ben a *Lityeraturnaja Gazeta*ban megjelent[179] egy cikk, amelyben a kibernetikát „a reakciósok tudományának", „divatos álteóriának" nevezték. Másutt is azt közölték, hogy „az új világháború uszítói a kibernetikát használják fel a saját mocskos gyakorlati munkáikhoz, hogy kidolgozzák az emberek tömeges megsemmisítésének új módozatait, azaz az elektromos és az automata fegyvereket".

Mindez azonban különösebben nem zavarta Kitovot abban, hogy még 1952-ben megszervezze a tüzérségi akadémián a számítógéposztályt. Az 1950-es évek végétől ez vált az első szovjet számítógépközponttá (VC–1 jelzés alatt, ez ma a védelmi minisztérium 27-es számú központi kutatóintézete). Kifejezetten ennek érdekében húzták fel a Horosevszkij úti épületet, amely nincs messze a védelmi minisztérium más katonai kutatóintézeteitől és a GRU főépületétől.

A VC–1 számította ki a világ első, a Szovjetunió által 1957-ben a világűrbe juttatott mesterséges holdjának keringési pályáját. Kitov alá több mint ezer embert kellett rendelni, de igazából nem volt honnan összeszedni őket: kibernetikus szakemberek nem léteztek még a szovjet főiskolákon. Ekkor a tudós elhatározta, hogy a műszaki főiskolák azon hallgatóit vonja be a munkába, akik képesek megírni a legegyszerűbb programokat, és ezt megtanítani a katonai szolgálatot végzők számára. Tulajdonképpen az utóbbi években így jár el az orosz védelmi minisztérium is, amikor ugyanezekről a műszaki főiskolákról vonja be a hallgatókat a „tudományos századokba".

„Hozzászoktunk mind a titoktartási rendszerhez, mind ahhoz, hogy a sorsunkat valahol valaki más dönti el – mesélte[180] a speciális állomány egyik hallgatója. – És mivel az államnak erre volt szüksége, csendben vártuk, hogy mi fog velünk történni."

Egy másik hallgató így emlékezett arra,[181] hogyan hívták be a műszaki egyetem évfolyamvezetőjéhez:



*– Kiváló tanulmányi eredményei alapján Kitov alezredes előzetesen kiválasztotta önt a szovjet védelmi minisztérium számítógépközpontjának létrehozását célzó munkára, hogy számítógépeken dolgozzon – mondta az évfolyamvezető.*

*– De mi ez? Még semmit nem hallottam róla.*

*– Az egész védelmi minisztériumon belül Kitovon kívül senki nem ért a számítógépekhez. Ne legyen gyáva. Ön nem egy buta ember – el fog tudni igazodni.*

Az újoncokkal találkozva Kitov elmagyarázta, hogy olyan „úttörőkké" kell válniuk, akik a hadseregen belül az elektronikus számítógépek fejlesztésén dolgoznak. A VC–1-ben végzett munka hasonló ahhoz, mintha folytatnák a tanulmányaikat: munkájuk végeztével, illetve annak ideje alatt Kitov *Az elektronikus számítógépek szabályozása*, *Az automatikus szabályozás elmélete*, illetve a *Halmazelmélet* című kurzusokat tartotta nekik. Az idő nagy részében a munkatársak programozással foglalkoztak, próbáltak kódokat írni, s minél rövidebb idő alatt azokat végrehajtani. A VC–1-ben dolgozták ki a GRU számára az első információs rendszert.

Kitov vált a szovjet hadászati informatika megalapítójává. Folyamatosan előadott a titkos kutatóintézetekben és publikált a hadügyi folyóiratokban. Átdolgozott anyagaiból végül két könyv született: az *Elektronnije cifrovije masini*, illetve az *Elementi programmirovanyija* (Elektromos számítógépek és a Programozás elemei). Később a Znanyije Kiadó megjelentette ezek egyszerűsített változatát is a szélesebb körű olvasóközönség számára.

Egyik könyvében Kitov kifejtette új elméletét, miszerint létre kell hozni az elektronikus számítógépek hálózatát az országok irányítására, valójában az első állami hálózatot a világon, olyat, amilyen később az internet lett. Projektjét Vörös könyvnek nevezte el. 1959 januárjában küldött néhány levelet az akkori pártfőtitkárnak, Nyikita Hruscsovnak, amelyben részletesen ismertette koncepcióját. Kitov úgy vélte, hogy a Vörös könyv lehetővé tenné, hogy a Szovjetunió felülmúlja Amerikát a számítástechnika terén,

maga a hálózat pedig megoldja mind a gazdasági, mind a védelmi feladatokat.

„Az egységes információs és számítógépes hálózat azt is lehetővé teszi, hogy gyorsan és hatékonyan gyűjtsük össze a feltétlenül szükséges statisztikai adatokat az egyes vállalatok helyzetéről, a rendelkezésre álló nyersanyagokról, pénzeszközökről, munkaerőről stb., és hatékonyan használjuk a feldolgozott eredményeket a gazdaság tervezéséhez és irányításához" – írta Kitov. A tudós olyan bunkerek létesítését is javasolta, amelyekben a számítógépközpontokat elhelyezhetik, s ezeket katonai irányítás alá kell helyezni. Kitov egyik tanítványa később azt állította, a Vörös könyv megvalósításához sokkal több erőforrásra lenne szükség, mint amennyit az atom- és űrprojektek együttesen felemésztenek.

Hruscsovhoz a levelek nem jutottak el. Hruscsov fia úgy emlékezett,[182] az ötlet nem nyerte el a központi bizottság ideológiai osztályának tetszését. Szuszlov „arról kezdett pusmogni", hogy a Vörös könyv miatt „a párt szerepe a mezőgazdaságban semmivé válna".

A szovjet védelmi minisztérium illetékes bizottsága közölte a munkatársaival, hogy „Kitov ajánlataiban nem állami, hanem bizonyos személyes, a karrierjére vonatkozó érdeket fedezett fel", és azzal vádolta a tudóst, hogy megpróbálta a védelmi minisztérium vezetését megszégyeníteni, illetve lebecsülni a Szovjetunió Kommunista Pártja (SZKP) vezető szerepét. Kitovot kizárták a pártból, elbocsátották, a vezető tisztségek betöltésétől eltiltották. Áttették az 5-ös számú tudományos kutatóintézetbe, ahol ettől kezdve katonai védelmi programok létrehozásával foglalkozott. Hamarosan megismerkedett Viktor Gluskov matematikussal, aki ától cettig elolvasta Kitov könyveit. Együtt szereztek tudomást arról, hogy az állam úgy határozott, beruház néhány olyan számítógép létrehozásába, amelyek teljes egészében az amerikai IBM-360-ast másolják.

* * *



1960. szeptember 6-án reggel a Szuvorovszkij körúton (ma Nyikitszkij körút), Moszkva központjában szokatlanul sok ember gyűlt össze. Egy kétemeletes családi háznál tíz újságíró várakozott, mellettük még több jelentéktelennek látszó férfi, akik a tömeget bámulták. Nem sokkal tizenegy óra előtt mindannyian az Újságírók Központi Házának termében gyűltek össze. Itt felment a színpadra és leült az asztalhoz két öltönyös ember, akik az amerikai Nemzetbiztonsági Ügynökség (NSA) munkatársaiként mutatkoztak be. Azért érkeztek a Szovjetunióba, hogy politikai menedéket kapjanak. Ez volt William Martin és Bernon Mitchell első nyilvános szereplése.

Néhány oldalas nyilatkozatukat Martin olvasta fel az egybegyűltek előtt.

*Szeretnénk közölni rokonainkkal, barátainkkal és mindazokkal, akiket érdekel, mi ösztönzött minket arra, hogy szovjet állampolgárságért folyamodjunk. Az amerikai Nemzetbiztonsági Ügynökségnél munkánk kezdetétől, 1957 nyarától meg voltunk győződve arról, hogy az USA kormánya szándékosan hazudik, nyilatkozatai tele vannak tévedésekkel, egyrészt saját politikájának az igazolása, másrészt a többi állam tevékenységének elítélése érdekében. Tudomást szereztünk arról, hogy az amerikai kormány az egyik szövetséges állam washingtoni nagykövetségén dolgozó kódolónak pénzt fizetett e szövetséges állam kódolt táviratainak megfejtéséért. Az ilyen és ehhez hasonló tevékenységek győztek meg bennünket arról, hogy az USA kormánya nem válogat az eszközökben, miközben ilyen módszerekkel a Szovjetunió kormányát vádolja. Azok közül, akik az (amerikai) védelmi minisztériumban, illetve az USA kormányának felderítő szerveinél dolgoznak, sokan tudják, hogy az állításaink helytállóak.*

A két amerikai férfi azt is elmondta, hogy beszédük szövegét nem egyeztették a szovjet kormánnyal, és úgy vélik, jobb lesz a Szovjetunióban élniük és a szakmájukban dolgozniuk, hiszen ebben az országban a nőknek több joguk

van, mint az Egyesült Államokban, a gazdasági és a politikai rendszer pedig az emberek érdekeit szolgálja.

Miután felolvasták nyilatkozatukat, Martin és Mitchell arról kezdtek beszélni, hogyan épül fel az NSA, hány munkatárs dolgozik ott. Kijelentették, hogy az ügynökség „ezer számítógéppel van felszerelve, annak érdekében, hogy az egész világ híreit kémlelje és lehallgassa." Ahogyan ők fogalmaztak, az amerikai titkosszolgálatok a külföldről érkezett magánlevelek nagy részét elolvassák.

*– Mit tudnak a Szovjetunió amerikai kémtevékenységéről? – kérdezte*[183] *egy amerikai újságíró.*

*– Amennyire én tudom, a Szovjetunió nem folytat légi kémkedést, ahogy azt az USA teszi – válaszolta Martin.*

*– Önök most mivel foglalkoznak?*

*– Oroszul tanulunk.*

Az Egyesült Államokban a szökevényeket árulóknak bélyegezték,[184] és a likvidálásukat követelték. Azután, hogy a kormányzat célzást tett rá, hogy az egyikük valószínűleg meleg, az amerikai sajtóban elkezdtek arról cikkezni, hogy homoszexuálisok fenyegetik a nemzetbiztonságot. Az újságok leginkább egyszerűen csak „közeli fiúbarátokként" utaltak rájuk.

Mitchell és Martin az 1920–1930-as évek fordulóján születtek, a nagy gazdasági világválság közepén. A hadseregben ismerkedtek meg, együtt szolgáltak Japánban. 1957-ben, amikor befejezték az egyetemet, matematikusként az NSA-hez verbuválták őket. A barátok rajongtak a sakkért, az orosz sakk-könyveket és azok feladatait búják, meg egy sakk-klubot látogattak, ahová időnként betért Valentyin Ivanov szovjet diplomata is.[185] 1959 decemberében Mitchell és Martin, a szökésre készülve Mexikóba, majd onnan Kubába repült, ahol a szovjet nagykövetség megbízottjaival találkoztak. 1960-ban szabadságot vettek ki, állításuk szerint azért, hogy meglátogassák a szüleiket, azonban többé nem tértek vissza az Egyesült Államokba.

Mire az NSA-ben észlelték a munkatársak eltűnését,



Mitchellt és Martint már senki nem tudta megtalálni. A hivatal belső vizsgálatot indított, amelynek során négyszázötven embert hallgattak ki, de a két férfi helyváltoztatásait csak Kubáig tudták követni. Egyikük házában találtak egy kulcsot, amely egy széfhez illett. Ebben volt a „Nyilatkozat" – ugyanaz, amelyet 1960 szeptemberében Martin felolvasott Moszkvában. Mivel szovjet kémekkel a vizsgálatot végzők semmilyen kapcsolatot nem találtak, úgy kombináltak, hogy szökésük oka személyes „anomáliáikban" keresendő: az NSA-nél egoistáknak, szociopatáknak, ateistáknak tartották őket. A titkos archívumban külön kiemelték: a szomszédok arra gyanakodtak, hogy homoszexuálisok.

A Szovjetunióban a két amerikai nevet változtatott, és egy tudományos kutatóintézetnél kezdtek el dolgozni,[186] matematikával és titkosítással foglalkoztak. Az NSA hírforrása azt közölte, hogy Martin – akit most már Vlagyiszlav Szokolovszkijnak hívtak – „gyógyíthatatlan alkoholista lett, csupa degenerált emberrel vette körül magát, és szexuális perverziókat folytatott".

1965 májusában a legkisebb információs egységeknek, a biteknek nevet adó Claude Shannon, vezető amerikai kódelemző és matematikus tartott előadást a LETI-n,* amely később tíz kibervédelmi szakembert bocsátott ki. Fellépése után odament hozzá Bernon Mitchell.

Miután bemutatkozott, Mitchell bevallotta, hogy jelenleg az FBI szovjet megfelelőjénél (bizonyára a KGB-nél) dolgozik, de Shannonnak csak néhány kérdést szeretne feltenni az előadás témájával kapcsolatban. A kérdésekből Shannon rájött, hogy Mitchell titkosítással foglalkozik. Beszélgetésük végén Mitchell azt is elárulta, hogy segíti a Szovjetuniót az Egyesült Államokkal folytatott információs háborúban.

* LETI = A Szentpétervári Állami Elektrotechnikai Egyetem orosz nevének rövidítése.

Az 1970-es évek végére Martin belefáradt a szovjet életbe és kérvényezte hazatérését, de az amerikaiak megtagadták a kérését, és megfosztották az állampolgárságától. Mexikóban halt meg az 1980-as évek végén. Mitchell Oroszországban maradt élete végéig, feleségül vett egy leningrádi zongoratanárnőt. Pétervárott halt meg 2001-ben, ott is temették el.

Ahogyan a titkosszolgálatok munkatársaitól megtudtam, épp az az információ, amit a két NSA-szökevénytől kaptak, adott lökést a szovjet vezetésnek, hogy ismét komolyan foglalkozzon a titkosítással és az információs védelemmel.

* * *

Az 1960-as években egy Kitov-tanítvány, egy bizonyos Viktor Gluskov vezette a kijevi Kibernetikai Intézetet. Csapatába fiatal, ambiciózus tanítványokat gyűjtött, hogy a Kitov-projekt, azaz a számítógép-hálózatok terjesztésének fejlesztésén dolgozzanak: amit korábban *Vörös könyv*nek neveztek, most hivatalosan „A számviteli és információfeldolgozás állami automatizált rendszere" néven futott (OGASZ).

Mint bármely más szovjet kutatóintézetben, itt is sokan foglalkoztak a munkájuktól távol eső ügyekkel. Kitalálták, hogy az intézetet nevezzék el Kibertonia országnak, saját alkotmányt, lyukkártyákból saját valutát alkottak. A kitalált államot a robotok tanácsa kormányozta, amelyet egy szaxofonos robot vezetett. A tudósok kiadták a *Vecsernij Kiber* (Esti Kiber) című lapjukat, és kiberkonferenciákat tartottak.

Gluskov elgondolása szerint az OGASZ szabályozni és gyorsítani lett volna hivatott a tervgazdálkodás döntéshozatali folyamatát. A fő számítógépközpont Moszkvában kellett hogy legyen, ezt kétszáz kisebb számítógépközponttal kapcsolták össze a régiókban. Ezek – telefonvonalon keresztül – az ország minden gyárával és vállalatával összekapcsolódtak volna, és a munkatársaik is közvetlenül érintkezésbe tudtak volna lépni egymással.

1970. október 1-jén Viktor Gluskov a Kremlbe ment egy döntő találkozóra a Politbüróval.* Az ülésen úgy határoztak, a projekt túlságosan sok pénzt igényel, és korai még belefektetni: a szovjet elvtársak másodjára utasították vissza a számítógép-hálózat létrehozásának kísérletét. Az Egyesült Államokban ekkor már működött az internet elődje, az ARPANET hálózat.

1970-ben Gluskov a feleségével, Galinával együtt (akit a barátai a „kibernetika anyjának" neveztek) a „rakparti házba" költözött,** majdhogynem a Kremllel szemben. A tudós előadásokat tartott műszaki főiskolákon a kibernetikáról, 1971-ben hivatalos kiküldetésre még Washingtonba is elutazott, onnan kérdezte meg a feleségét, milyen kabátot szeretne. „Velúrbőrt nercgallérral, vagy inkább olyat, ami szintetikus anyagból készült? Vologyának [a fiának] és neked szintén lehet átmeneti a kabát – írta Gluskov a feleségének. – Most este van, a szállodában ücsörgök, és azokat a műszaki anyagokat nézem át, amelyeket napközben kaptam; tévézek és alszom."

1980-ban Anatolij Kitov fia, Vlagyimir feleségül vette Gluskov lányát, Olgát, így a vezető szovjet kibernetikusok családjai rokonságba kerültek. 1985-ben, amikor a fiatal Mihail Gorbacsovot választották meg pártfőtitkárnak, Gluskov ismét felajánlotta terveit a hatalomnak. Ezt felelették neki: „az SZKP Politikai Bizottságának más funkciói vannak, mint a népgazdaság irányításának automatizálása." Ezután a tudós ideje nagy részét a dácsáján töltötte. 2005-ben halt meg.

* A Szovjetunió Kommunista Pártja (SZKP) Politikai Bizottsága, a legfelsőbb párttestület.

** Ez az épület a kiemelt káderek elhelyezésére, egyúttal közvetlen megfigyelésükre szolgált. – *A szerk.*

*27. fejezet*

## A „Kvantum" és a „Galilei"

A katonai kutatóintézetek, amelyeket jórészt Kitov és Gluskov elképzelései alapján hoztak létre, mostanra az orosz kiberhadseregek bázisai lettek. A tudományos századokba ugyanazon elvek alapján toboroznak, amelyek szerint egykor Kitov vette fel a munkatársait. A 27-es számú központi kutatóintézetben (CNII-27) – így nevezik most az egykori 1-es Számítógépközpontot – jelenleg az informatikai védelem eszközeit gyártják. Ugyanitt található a védelmi minisztérium számára fontos új programok befogadási eljárását végző központ is. Ide folyamatosan keresnek tudományos munkatársakat hadiinformatikai technológiák kidolgozására, tíz-húszezer rubeles fizetéssel. Néhány évig a CNII-27 része volt a CNII-16-nak, ahol a különleges kommunikációs hálózatok biztonságát tanulmányozzák.[187]

A CNII-27-hez hasonló központokban gyakran alkalmaznak hekkereket, és állítólag kiváló szakembereket. Interjúalanyaim néhány intézetet külön kiemeltek: a Kvantum kutatóintézetet, a 26165-ös katonai részleget, a 74455-ös katonai részleget, az Atlasz tudományos és gyakorlati központot, az FSZB №1 tudományos-mérnöki vállalatot, az Echelon kutatóintézetet és másokat. Tucatnyi intézetben foglalkoznak információbiztonsággal, ezekben ezer ember dolgozik, akik a belépésükkor rendszerint egy nyilatkozatot is aláírnak a titkos információkhoz való hozzáférés rendjéről.

A moszkvai Hovrino kerület kies részén áll egy négyemeletes, szürke, kopott téglaépület, minden különösebb ismertetőjel nélkül. Szögesdrót kerítés veszi körül, a földszinti ablakokat fehérre mázolták, némelyikre ibolyaszínű védőfóliát ragasztottak. Az épület mellett ipari terület és vasút húzódik. Véletlenül biztosan nem téved ide senki.



Ebben a téglaépületben található a Kvantum kutatóintézet. 1978-ban annak az ipari automatikai tervezőirodának a bázisán jött létre, amely az első szovjet számítógépet gyártotta. Jelenleg a Kvantum alapvető tudományos központnak számít a speciális rendeltetésű számítógépes és informatikai védelmi rendszerek létrehozásában. „Az intézmény tevékenysége állami jelentőséggel bír" – mutatnak rá[188] a kutatóintézet honlapján. Néhány oroszországi kibervédelmi szakember kérdésemre azt mondta, hogy ők a Kvantumban a kiberfegyverkezés kutatásával foglalkoznak. Az egyik orosz hekker azt mesélte, hogy ide az információs védelmi karok „nem fecsegő" végzett növendékeit hívják dolgozni.

2008-ban a Kvantum átkerült[189] az FSZB vezetése alá. Ekkor már harmadik éve igazgatóhelyettesként dolgozott itt a titkosszolgálatoktól érkező Georgij Babakin: 1998-ban fejezte be az FSZB titkosítási akadémiáját, 2005-ig energetikai hivatalokban dolgozott.

2011. április 1-jén Babakinhoz tapintatos levél érkezett[190] Olaszországból. Marco Bettini küldte, a Hacking Team cég munkatársa. A levélhez Bettini néhány fájlt csatolt: egy segédkönyvet a Remote Control System (RCS) nevű programvírus használatához, ennek demóverzióját, és hivatkozásokat a letöltéséhez.

A Remote Control System (ekkor még Galileinek hívták a programot) a megfertőzött struktúrákon lehetővé teszi a végrehajtott összes művelet követését: képernyőképet készít, irányítja a webkamerát és a mikrofont, „elfogja" a levelezést a messengeren és az elektronikus postán, felismeri, hogy milyen billentyűket nyomott le a számítógép vagy az okostelefon tulajdonosa. Mindezen adatokat célkérdőíven gyűjtötték – az RCS tulajdonosai ezeket jól láthatták a felhasználóbarát felületen. A programot legálisan, több

százezer dollárért árulták és árulják,[191] és a világ legtöbb országában meg is vették (Nigériától és Ugandától kezdve az Egyesült Államokig és Olaszországig), hogy a bűnüldözés elleni küzdelmet tökéletesíthessék. Április 4-én Bettini küldött még egy levelet az orosz férfinak: „Kipróbálta a demót? Milyen? Kérem, jelezze, hogyan készül a fertőzésre. Mit gondol, kinek küldjem az árazást, Önnek vagy az Infotekszneк?"*

Babakin azonnal válaszolt: „Letöltöttem, köszönöm. Az Infotexszel azon dolgozunk, hogy telepítsük a demót és kapcsolódjunk az Önök szerveréhez. Az értesítéseket nekem és az Infotekszneк is küldheti, partnerek vagyunk. Igaz, úgy gondolom, hogy ők nem használják az PGP-t, így én mindent át fogok küldeni nekik ☺".

Április 5-én Babakin ismét írt Bettininek. „Lesz ideje egy májusi prezentációra Moszkvában?" – kérdezte az olasz férfitól.

Minden valószínűség szerint a programok FSZB számára történő prezentációjáról volt szó. Egy másik levelezés arra mutat rá,[192] hogy a fenti párbeszéd után egy hónappal az RCS-t az energetikai hivatalok munkatársai két különböző csoportjának is prezentálták az orosz fővárosban. Megmutatták nekik, milyen program tudja követni a fertőzött notebookokat. „Az [FSZB] reakciója igen pozitív volt, érdeklődtek a lehetőségekről. Kérdéseikből világossá vált, hogy van tapasztalatuk a legális feltörések terén, de nyilván nincs lehetőségük megfertőzni a mobilkészülékeket és a Maceket" – jegyezte meg levelezésében a Hacking Team képviselője.

A 2012-2014 közötti években az Infoteksz, a Kvantum nevű kutatóintézet képviseletében az olasz cégnek négyszázötvenegyezer eurót fizetett.[193] Később a cég bejelentette,[194] hogy megszerezte az RCS-t, annak érdekében, hogy

* A védelmi programok kidolgozója a titkosszolgálatok vagy a védelmi minisztérium számára. – *A szerző.*



„a gyakorlati informatikai védelem terén emelje a kutatások színvonalát".

„Az állami vállalatok és szervezetek, bármit is vettek a Hacking Teamtől, azt a kémkedés érdekében vették – erősíti meg egy kibervédelemben vezető pozícióban álló orosz cég szakembere. – Támadhatóságot nem az infrastruktúra védelme számára vásárolnak, hanem az aktív intézkedésekhez."

2013-ban Georgij Babakin eljött a Kvantumtól, hogy az MTSZ* információbiztonsági ügyosztálya projektjeit vezesse. Ezt a mobilszolgáltató cég képviselője, Dmitrij Szolodolnyikov erősítette meg. Az orosz ellenzékiek kitartanak amellett, hogy az MTSZ együttműködik a titkosszolgálatokkal. 2016 áprilisában az orosz ellenzéki Oleg Kozlovszkij és a Korrupcióellenes Küzdelem Alapítvány munkatársa, Georgij Alburov azzal vádolta[195] az MTSZ-t, hogy részt vett Telegram-fiókok feltörésében: ismeretleneknek sikerült megkaparintaniuk a feltörés áldozataitól a belépéshez szükséges autorizációs kódokat, amelyeknek sms-ben kellett volna megérkezniük (de nem kapták meg). Kozlovszkij később elmondta, hogy az MTSZ a feltörés pillanatában kikapcsolta az sms-szolgáltatást. A vevőszolgálatnál közölték vele, hogy ezt a cég műszaki biztonsági osztálya hajtotta végre. Később az aktivisták kiposztolták a 2016. áprilisi szolgáltatásokról szóló nyugtákat: ezek mind Kozlovszkijnál, mind Alburovnál az sms-szolgáltatás kikapcsolását bizonyították.

* * *

Az információbiztonság fejlesztésével és kutatásával foglalkozó orosz katonai kutatóintézetek tevékenysége szinte teljes mértékben titkos. A munkatársak írásban vállalnak titoktartási kötelezettséget, ráadásul gyakran tarthatnak attól is, hogy az állam megfigyeli őket. Az Ukrajnában

* Az egyik legnagyobb orosz telekommunikációs társaság nevének rövidítése.

elhunyt orosz katonák szülei még az újságírókkal való érintkezést is elutasították. Én elutaztam néhányukhoz, láttam fiaik sírját a védelmi minisztérium koszorújával. De a rokonok elzavartak, amikor ellátogattam a szülőkhöz, elzavartak, kérve, hogy soha többé ne jelenjek meg náluk. Államtitoksértéssel kapcsolatos büntetőügyeket egyre gyakrabban indítanak az utóbbi években Oroszországban – akár a legártatlanabb okokból. Például 2015 januárjában a vjazmai Szvetlana Davidovát hazaárulással vádolták.[196] Az FSZB szerint 2014-ben Davidova felhívta Moszkvában az ukrán nagykövetséget, hogy közölje: Ukrajnára ráirányították a háza mellett állomásozó katonai egységet. Davidova két hónapot ült a lefortovói börtönben, ezt követően a büntetőügyét megszüntették, valószínűleg azért, mert túlságosan felkeltette a közvélemény figyelmét.

Arról, hogy mi folyik a katonai intézetekben, és hogy ott pontosan mivel foglalkoznak, csak a ritkán megjelenő hírekből lehet tudni. 2012-ben az FSZB egyes számú kutatóintézete, amely a Moszkva melletti Zseleznodorozsnijban található, a rejtjelezés tanulmányozása céljából megpróbált[197] törvénytelenül mikroelektronikát vásárolni az Egyesült Államokban. Korábban ugyanez az intézet „a beszédelemzés és -feldolgozás antropomorf módozatait", „a személy hang alapján történő automatikus felismerését", „az adott személy hangjának változtatási és utánzási képességeit" kutatta.

Olykor a haditudósok maguk beszélnek a kutatásaikról. Az Eselon kutatóintézet egyik 2013-as jelentésében[198] részletesen beszámolnak a külföldi számítógépes programok támadhatóságának kereséséről, rámutatva, hogy olykor rejtett funkciók jeleire bukkannak a termékekben és készülékekben, de a hasonló fenyegetések esetén az ellenlépésnek az az egyik módja, ha a tanúsítási tesztek során ellenőrzik a programkód biztonságosságát. Állami objektumok biztonságának védelmére szakosodott interjúalanyom véleménye szerint ezen foglalatosságoknak nem



lenne értelmük. A lényeg az, hogy a gonosz amerikaiak ne küldjenek kémeszközöket tartalmazó berendezéseket. Ezeket a felszereléseket állítólag ellenőrizték, és az állami vállalatokhoz viszonteladás útján kerültek. Azonban ez egyenlő a csalással, mert lehetetlen ezeket az ügyleteket ellenőrizni – magyarázza a hírforrás. – Ráadásul ők ezt támogatás nélkül és a frissítések késleltetésével adják el. És ott állnak az ilyen számítógépek a zárt rendszerhez tartozó szobákban, de mindegyik tele van biztonsági réssel."

A kutatóintézeteknél magasan képzett emberek dolgoznak – erre a Kvantum történetéből is rá lehet jönni. „A legtöbb kutatóintézet rendelkezik méregdrága programokkal hivatalosan a »behatolások tesztelésére«, de ezeket valójában a feltörésekhez használják – folytatja a beszélgetőtársam. – Ez egy grafikus felület egy halom exploittal. Általában az ilyen dolgokat az FSZB-nek veszik meg. Évente több ezer dollárba kerül egy ilyen, de a kutatóintézeteknél ezeket mintha nem is használnák, inkább titkosszolgálati érdekből tartják őket, hogy megértsék, milyen támadásokra lehet számítani."

A hekker úgy mesélte el nekem ezt a történetet, hogy felalá járkáltunk egy forgalmas út kereszteződésénél – könnyen el lehetett tűnni, és egy árva lélek nem járt arra: ha mégis meg akarnak figyelni bennünket, azt azonnal észrevesszük.

Szerinte a munkaerőpiacról sok programozót hívnak a „hivatallal kapcsolatban álló" kutatóintézetekhez dolgozni. Az egyik jelentkezővel folytatott felvételi beszélgetés során utaltak rá, hogy az egyik legelterjedtebb programnál nulladik napi támadhatósági pontokra bukkantak.

* * *

2017. május 5-én, egy nappal a franciaországi elnökválasztás előtt, a Wikileaks közölte Emmanuel Macron és stábja feltört archív levelezését. A választáson vele szemben Marine Le Pen állt, a Nemzeti Front jelöltjeként. A kampány

időszakában Le Pen találkozott Vlagyimir Putyinnal. Le Pent nem egyszer érte az a vád, hogy túl szoros viszonyt ápol Oroszországgal. Mintha megismétlődtek volna a 2016. őszi amerikai események: az elnökségért folytatott kampány időszakában a hekkerek feltörték Hillary Clinton munkatársainak postáját, miközben Putyin és a republikánus jelölt, Donald Trump egymásnak küldözgette bókjait.

Macron 9 gigabájtos postája párttagok és a választási stáb munkatársainak levelezését tartalmazta, sőt néhány pénzügyi dokumentumot is. Az egyik levél arra hívta fel a figyelmet, hogy Macron nagyon beteg. Emellett szinte azonnal kiderült,[199] hogy kilenc fájlt egy bizonyos Georgij Petrovics Roska nevű felhasználó megváltoztatott.

Georgij Petrovics Roska programozó az Evrika részvénytársaság munkatársa volt.[200] Az Evrika programvédelem fejlesztésével foglalkozott a védelmi minisztérium és a titkosszolgálatok megbízásából, és egyebek között a Kvantum megrendeléseit is teljesítette. Az Evrika társtulajdonosának birtokában van egy lakás is[201] egy olyan házban, amelyben Vlagyimir Putyin közvetlen hozzátartozói laknak.

A *Párhuzamos számítógépes technológiák* című arhangelszki szakmai konferenciára Georgij Roska együtt utazott Szergej Zajcevvel, aki a védelmi minisztérium speciális fejlesztések centrumának munkatársa. Rajtuk kívül a konferenciára érkeztek a Kvantum katonai részlegének elektronikus felderítést végző munkatársai is. Maga Roska a konferencia programjában úgy szerepelt, mint a 26165-ös katonai egység szakembere – az intézmény a vezérkar különleges szolgálatának 85-ös számú kiemelt központját rejti Moszkvában, a Komszomolszkij sugárúton, a 19. század elején épült Hamovnyicseszkij kaszárnya történelmi épületében. A katonai részleget hosszú évekig Szergej Gizunov ezredes vezette, aki kiválóan ért a rejtjelezéshez. Az utóbbi években a GRU (a Felderítő Főcsoportfőnökség) vezetőhelyetteseként dolgozik. 2016-ban az Egyesült Államok felvette a nevét a szankciós jegyzékébe, azzal gyanúsítva, hogy hekkertámadásokban vehetett részt.

Pontosan a Hamovnyicseszkij kaszárnyaépületéből utazott taxival a repülőtérre Alekszej Morenec, akit 2018-ban azzal vádoltak,[202] hogy támadást kísérelt meg egy vegyi fegyverek betiltásáért küzdő szervezet ellen Hollandiában. Ugyanott, a Komszomolszkij sugárúton – az amerikai ügyészek szerint – a GRU tíz hekkere és egyéb munkatársa dolgozott,[203] akik, ahogyan azt az amerikai hírszerzés véli, megtámadták az amerikai Demokrata Párt nemzeti bizottságának szerverét.

*28. fejezet*

## A titkosítás katonái

Az orosz számítógépes társaságok és titkosszolgálatok – a GRU, az FSZB CIB, a Belügyminisztérium „K" ügyosztálya – vezetőinek nagy többsége az FSZB titkosírási, informatikai és hírközlési akadémiáján tanult (1991-ig ez a KGB felsőoktatási intézményének 4-es számú műszaki kara volt). 1987-ben végzett matematikai mérnökként ugyanitt a Kaspersky Lab megalapítója, Jevgenyij Kaszperszkij. Itt tanult Georgij Babakin is, aki később a Kvantum kutatóintézetet vezette. Az akadémia végzett növendékei közé tartozik néhány aktív hekker is, akikkel akkor találkoztam, amikor anyagot gyűjtöttem ehhez a könyvhöz.

Mihail Maszlennyikov, a KGB felsőoktatási intézetének egyik végzett hallgatója úgy nyilatkozott,[204] hogy az oktatás *A 22-es csapdájára** hasonlított. A 4-es számú kar, amely a titkosírásra specializálódott, a Bolsoj Kiszelnij keresztutcában, a Lubjankán egy családi házban volt (mostanra az akadémia átköltözött a Micsurin sugárút modern épületébe). A díszterem bejáratánál egy plakát függött: *You are welcome.* (Üdvözlünk!) Az oktatók ellenőrizték a hallgatók külsejét és frizuráját. Az alapkiképzésen gyakran hangzottak fel az ehhez hasonló frázisok: „A melletted álló elvtárs felfigyelt rá, hogy nem borotválkoztál", „A sorban egyformának kell lenni, mert éppen ettől különbözik a sornélküliségtől". A matematikus-kódolókhoz úgy viszonyultak,

* Szállóige, az abszurd, kölcsönösen kizárható követelményekre értendő, a kifejezés az azonos című, háborúellenes Joseph Heller-regényből származik. – A szerző megjegyzése.



mint az átlagos katonákhoz, akiknek elsősorban tiszta csizmájuknak kellett lennie, a kódok és formulák csak ezután következtek.

A matematikaianalízis-előadásokon a hallgatóknak arról beszéltek, hogy következetesen kell haladni, kis lépésekben (mint a programozóknak, akiknek a munkája során a kódok sorai folyamatosan kapcsolódnak össze a nagy programmal). Olykor a matematikusok kimentek a „terepre" dolgozni, mint az átlagos ügynökök: elvegyültek a sok embert vonzó rendezvények tömegében, hogy előre kiszagolják a „lehetséges incidenseket". Amikor 1977. január 8-án Moszkvában robbantásos merényletet követtek el (hét ember életét vesztette, körülbelül harminc megsebesült, a bűncselekménnyel az Örmény Nemzeti Egységpártot vádolták), a hallgatóktól megvonták az újévi szünetet: napokig azt a metróvonalat kellett járniuk, ahol az egyik robbantás történt, hogy „elhárítsák a terrortámadásokat".

Az oktatás ideje alatt gyakran hallottak előadásokat a sikeres kódfejtő műveletekről, amelyeknél az amerikai Nemzetbiztonsági Ügynökség volt a minta a Szovjetunió titkosszolgálatai számára. Az előadások közötti szünetekben a hallgatók közül sokan elvonultak a könyvtár félreeső, titkos dokumentumok tanulmányozására kijelölt sarkaiba, hogy preferánszot játszanak: a kártyajátékot matematikai jellege miatt szerették, mivel lehetőséget ad a különböző variációk kiszámítására.

A KGB felsőoktatási intézményének elvégzése után Maszlennyikov a KGB 8-as számú intézetébe került: ez volt az amerikai Nemzetbiztonsági Ügynökség szovjet megfelelője. Kétszázötven rubelben határozták meg a fizetését, ami kétszer annyi volt, mint egy kezdő kutatóé bármely más intézetnél. Az intézetben folyamatosan arról volt szó, hogy a legfőbb feladat egy új kódolóapparátus létrehozása.

A munka reggel kilenckor kezdődött, de már két óra múltán megkezdték az „ötperces testnevelést", amikor is

sakkoztak. Hamar eljött az ebédidő, a továbbiakban pedig a munkanap végét várták. Mindez nem sokban különbözött más szovjet intézetek hétköznapjaitól. „Órákig nem másztak elő a dohányzóhelyiségből, egyik anekdota követte a másikat, és mindenről tárgyaltak, amiről csak akartak: a hokiról, a tévében épp futó filmről, az intézeti pletykákról, arról, hogy mit hol lehet beszerezni (szabadon vásárolni bármilyen normális dolgot ezekben az években lehetetlen volt), zoknikat és pulóvereket kötöttek, a boltokba szaladgáltak – emlékezett vissza a KGB felsőoktatási intézetének egyik végzett hallgatója. – Munka mint olyan szinte sehol sem folyt, mindenütt a szürkeség és az unalom uralkodott, ami fokozatosan közömbösségbe és iszákosságba torkollott." Olykor a matematikusokat átcsoportosították a rejtjelfejtéstől a külföldi turisták megfigyelésére, így történt az 1980-as moszkvai olimpia idején is.

Amint azt Maszlennyikov felidézi, a 8-as számú KGB intézet szinte felhagyott a munkával, amikor megjelentek náluk azok a számítógépek, amelyekre fel lehetett telepíteni a videójátékokat. A leginkább a *Space Quest* 2-val foglalkoztak, az egyik első, kalandokat ígérő számítógépes játékkal, amelynek hőse különböző bolygókra kerül. Annak kitárgyalására, hogyan megy keresztül a lápon a szörnnyel együtt, teljes munkanapok mentek rá. A kriptográfusok sémákat rajzoltak az átkelési szintekről, és egymással vitatkoztak. Csak egy hét elteltével vették észre, hogy a főnököt meg lehet kerülni úgy, hogy a bokrok közé bújnak, és leeszik róluk a bogyókat.

Amikor 1991. augusztus 19-én az úgynevezett Állami Bizottság (GKCSP)* rendkívüli helyzetet kihirdetve magához ragadta a hatalmat az országban, a KGB összes munkatársát a szolgálat szigorított rendjébe helyezték. Hamarosan közölték velük, hogy a KGB támogatja a GKCSP-t, ám a puccs kudarcot vallott, a hivatal vezetőségét letartóztatták, és a KGB-ben tömeges elbocsátások kezdődtek. Távozott Maszlennyikov is. Azt mondja, sok titkosírási algoritmus és az intézet más fejlesztései, amelyeken dolgozott, elvesztek, és ezeket senki sem szabadalmazta.

* A Rendkívüli Állapot Állami Bizottsága (GKCSP) 1991. augusztus 19-én jelentette be, hogy átvette a hatalmat Mihail Gorbacsovtól, de az államcsíny néhány nap alatt összeomlott, és a puccsisták szándékával szemben éppen hogy felgyorsította a Szovjetunió felbomlási folyamatát.



Mindazonáltal a titkosírási főiskola a titkosszolgálatok kötelékében folytatta munkáját, immár abban a struktúrában, amelyet 1992-ben Oroszország védelmi minisztériumának akadémiáján hoztak létre (ez most az FSZB akadémiája). Az egyik ott végzett hallgató mondta el, hogy az 1990-es évek elején egy átlagos iskolában tanult Moszkva déli részén. Időnként meglátogatták az iskolát a titkosszolgálat munkatársai, jelentkezési lehetőséget ajánlva az akadémiára. Egyszer a fizikaóra rovására érkeztek. A két titkosszolgálati munkatárs nemcsak stabil munkát, hanem sok kalandot is ígért az akadémiai végzettséget szerzőknek. A fiatalember elgondolkodott, és eldöntötte, hogy a következő találkozáskor a részletekre is rákérdez. Erre csak egy év múlva került sor: miután tudomást szereztek a fiú matematikai sikereiről, az állambiztonsági tisztviselők felajánlották neki, hogy jelentkezzen a titkosírási akadémia intézetébe.

Két vizsgát tett le matematikából: írásbelit és szóbelit, írt egy esszét, és összegyűjtötte a bejutáshoz szükséges pontokat. A vizsgák után minden rokonát az akadémiához tartozónak számították. Az ottani rend katonai jellegű volt: kemény napirend, lövészeti tanfolyamok, emellett az idő több mint fele matematika-előadásokra és szemináriumokra ment el.[205] Az 1990-es évek elején a főiskola ugyanolyan hanyatlást élt át, mint az egész orosz állam. Az egyik oktató a késő szovjet időkre olyan időszakként emlékezett vissza, amikor a főiskolán a legjobb matema-

tikusok és kódolók dolgoztak. Mások azt mesélték, hogy a titkosírással és a kódvisszafejtéssel foglalkozó kurzusok azokra a munkákra is támaszkodtak, amelyeket az amerikai Nemzetbiztonsági Ügynökség egykori szökevényeitől kaptak.

Hogy felkutathassák az újabb potenciális hallgatókat, 1991-től az FSZB titkosírás-olimpiákat rendezett a tanulók körében. Az ifjú hekkereket a titkosszolgálatnál manapság is keresik.

*29. fejezet*

## Az FSZB ifjú programozói

2015-ben a Moszkvai Kadétiskolában, amely Moszkva déli részén, a Kolomenszkaja metrómegállóhoz közel helyezkedik el, megalakult az „Oroszország FSZB-jének Ifjú Programozói" nevet viselő kör.

Ebben 9–11. osztályos tanulók vettek részt. A kört Szergej Epifancev informatikatanár szervezte. Azt mondta, „a projektet azért hozta létre, hogy „szembeszálljon minden »ukrópaival« (azaz ukrajnaival), az összes marhával, aki az amerikai életformát támogatja, szembeszálljon az »ötödik hadoszloppal«, mindenkivel, aki ellensége a jelenkori Oroszországnak". Az ő diákjai „ott lesznek az új orosz IT-ipar startjánál", elnökünk megfogalmazása szerint „a külföldi programbiztonság alól felszabadulva". Mint Epifancev írta,[206] ő „a bűnüldöző szervek számára készíti fel a jövő információbiztonsági specialistáit".

Epifancev a tanulókört az FSZB Határvédelmi Múzeumának és a Haderő Központi Múzeumának támogatásával alapította – 2015-ben a diákok ezeknek az intézményeknek fejlesztettek ki szoftvert. A Központi Múzeum igazgatóhelyettese, Vaszilij Afanaszjev ezredes megerősítette,[207] hogy ők támogatják a projektet.

A kadétiskola weboldalán található részletes bemutatóanyagból[208] kiderül, hogy az „ifjú programozók" az információs biztonság alapjairól szóló kurzusok során megtanulják, hogyan telepítsék fel és használják a sebezhető programokat, és hogyan hajtsanak végre DDoS-támadásokat. Foglalkoznak a postafiókok jelszavainak Brute-force alapú feltörésével, a nyilvános wifik támadhatóságának

vizsgálatával (a moszkvai metró wifijének példáján) és a telefonbeszélgetések rádión keresztüli lehallgatásával is (beleértve a drónok nyújtotta segítséget). Ezeket a kutatásokat 2017 februárjáig együtt végezték az MIFI* számítógépes rendszerek és technológiák tanszékével.

2016 decemberének végén az ifjú programozók részt vettek[209] a Moscow CTF School nevű versenyen, amelyre katonai egyenruhában érkeztek.[210] Negyedik helyezést értek el. Az egyik hekker, aki a CTF állandó résztvevője, azt mondta, a rendezvény kiemelt színhelye az informatikai biztonság szakemberei számára nyújtott titkosszolgálati munkaajánlatoknak: a hekkerekhez odamennek a szünetben, prospektusokat osztogatnak nekik, és elhívják a diákokat tájékoztató beszélgetésekre.

A versenyt, amelyen részt vettek az ifjú programozók, a védelmi minisztérium különleges fejlesztési központja (CSZR) támogatta, és riportalanyaim szerint a leggyakrabban innen toborozzák az információs védelem szakembereit. A védelmi minisztérium 2014-ben alapította a CSZR-t, ahová a műszaki egyetemet végzettek köréből kerestek munkaerőt. A betöltetlen álláshelyek azt mutatták, hogy a legtöbb munkatársra a védelmi minisztérium CSZR-ében az exploitok analíziséhez (ez a számítógépes támadások végrehajtására szolgáló program) és *reverse engineering*re (a programok és eszközök működésének és funkcióinak forráskódból történő megismerése, visszafejtése) volt szükség. Egy kódtörő, akinek a CSZR-nél állást ajánlottak, azt mesélte, a titkosszolgálatoknál végzendő munkáról csak néhány hekkerrel és kereskedelmi cégnél dolgozó szakemberrel sikerült megállapodni, mert sokuk nem akarja, hogy korlátozzák külföldi utazásaikat.

A kadéti testület weboldala rámutat,[211] hogy a verseny után, 2016 decemberében, az ifjú programozók informális

* A moszkvai Nemzeti Nukleáris Kutatási Egyetem nevének rövidítése.



körülmények között kapcsolatba léptek az FSZB munkatársaival, akik „nagyra értékelték a tanulók felkészítését", és „elismerték [a tanulók] perspektíváit országunk kiberbűncselekmények és kibertámadások elleni védelmi képességének fejlesztésében".

Annak érdekében, hogy bármit is megtudhassak Epifancev projektjeinek működéséről, regisztráltam az fsb.ru.com weboldalra. A főoldalon Epifancev fotója szerepelt,[212] háttérben az FSZB címerével. Ugyaninnen egy link mutatott a projekt ismertetőanyagára,[213] amely arról tanúskodott, hogy Epifancev együttműködik a védelmi minisztériummal és az FSZB-vel.

2016. január végén az ifjú programozók meghallgatták az FSZB munkatársa, Oleg Krzsizsanovszkij előadását a jelenkori háborúkról.[214] „A háború már közeleg – tért ki a lényegre Krzsizsanovszkij mindjárt az előadása elején. – Minimum két fronton, mivel Ukrajnában és Szíriában is jelen vannak a katonai szolgálatot teljesítő embereink." Ezután kijelentette, ha „izolálnánk a harminc legnagyobb hatalommal bíró zsidót, akkor véget érnének a háborúk", ám a folyamatokat a világon többnyire az olyan vállalatok irányítják, mint a General Motors, a Shell, a Coca-Cola vagy a McDonald's. „Általában véve milyen is a háború? A következő sztereotípiák élnek erről: tankok, gyalogság, szuronyrohamok, lövészárkok. De nem lesznek többé ezek a megszokott, fronton zajló háborúk. A védelem területén a közelmúltban vezették be a »hibrid háború« terminust. Mit gondolnak, mit jelent ez?" – kérdezte Krzsizsanovszkij. „Az interneten zajló kiberháborút. Fel lehet törni egy másik állam weboldalait, meg lehet nézni az onnan származó információkat, és ezeket fel lehet használni ellene" – válaszolta az ifjú programozók egyike. „Helyes!" – mondta a tanár. „Meg amikor ötletek cserélnek gazdát a tömegmédián keresztül – vetette fel egy másik tanuló. – Vagy amikor a kémhálózatok tüntetések megszervezésével ráveszik a népet arra, hogy döntse meg a kormányát." „Helyes! Itt

említeném meg még a terrorcselekményeket mint eszközt a nép bizalmának megingatására – mondta Krzsizsanovszkij. – És létezik még egy átfogó módszer az erőszakmentes ellenállás terén is."

Krzsizsanovszkij, aki az FSZB múzeumában dolgozik, disszertációját *A katonai szolgálat motivációinak kialakulása a toborzási életkor előtt álló fiataloknál a hadtörténeti múzeum szociokulturális tevékenysége folyamatában* témában védte meg.[215] A diákoknak a „narancsos forradalomról" beszélt, és arról, hogyan játszódott le tragédia Líbiában, amikor meggyilkolták a törvényes vezetőt, Moammer Kadhafit. „Akkor vajon miért nem egyesültünk mi mindannyian, és támadtuk meg Amerikát?" – kérdezte az egyik tanuló.

A múzeumi találkozásokon kívül a tanulók az Egységes Oroszország Párt „fiatal gárdája" aktivistáinak versenyeit látogatják,[216] és meghallgatják a Szövetségi Nyomozó Bizottság vezetője, Alekszandr Basztrikin felszólalásait,[217] illetve Vlagyimir Putyin portréjával fényképezkednek.[218] A tanulók lefordítottak egy amerikai hekkerről szóló könyvet,[219] aki hitelkártyaadatokat lopott el és pedofilokat leplezett le (a tanulók őt Teszak-hekkernek nevezik, valószínűleg az Occupy Pedophilia mozgalom alapítójára, Makszim „Teszak" Marcinkevicsre utalva). A könyvben, egyebek mellett, részletesen tárgyalják a titkosszolgálatok munkáját az informatikai védelem területén. Elért eredményeikért az ifjú programozók tíz oklevelet kaptak,[220] az egyik diák 2015 augusztusában méltónak találtatott[221] a „CSEKA–KGB–FSZB 95 éve" jelvényre is.

A diákok zenét is tanulnak a kadétiskolában, ezért zenés videóklipeket is szoktak forgatni: 2017 tavaszán felvették[222] a „2018-as futball-világbajnokságra az orosz válogatott himnuszát", amelyet a CSZKA telephelyén mutattak be.[223] A kadétok készítettek videókat a szélsőséges nézetekkel szemben is. Az egyiknek az utolsó snittjén[224] az „ifjú programozók" és Epifancev tréfából náci üdvözlésre lendítik a karjukat. A felirat: *Ugye, milyen vicces?*



Azt Epifancev megtagadta, hogy a munkájáról eláruljon nekem bármit is. „Nem kívánok önnel beszélgetni" – jelentette ki. Epifancev harminchét éves, a Moszkvai Állami Bölcsészettudományi Egyetem informatika szakán végzett. A kadétiskola előtt Noginszkban dolgozott[225] egy különleges intézet igazgatóhelyetteseként, és a hazafias katonai klubot, a Fakelt* vezette. Itt végzett munkájáért köszönetben részesült az FSZB golicini határőrképző főiskolájától. A moszkvai oktatásért felelős ügyosztály weboldala szerint[226] Epifancev háborús veterán, emlékérme van „a szovjet csapatok Afganisztánból való kivonulása huszonöt éves évfordulójára", illetve jelvénye „Az oroszországi FSZB műveleti-kutatási hivatala kilencvenöt éve" felirattal.

Megpróbáltam kapcsolatba lépni tíz ifjú programozóval a közösségi médián. Többségük látta az üzeneteket, de nem válaszolt. Az egyik diák először beleegyezett az interjúba, de egy idő után szintén nem válaszolt. Azután, hogy megpróbáltam felvenni a kapcsolatot a diákokkal, Epifancev írt rám: „Maga mindegyiktől sorban ki akarja erőszakolni az interjút? Milyen alapon kérdez gyerekeket? Kérem, hagyjon minket békén."

2017. május 25-én az ifjú programozók köre szerződést írt alá a kölcsönös együttműködésről az FSZB Akadémiájával és a moszkvai FSZB hivatallal.

* A szó fáklyát jelent. – *A fordító megjegyzése.*

*IV. rész*

# Háború

*30. fejezet*

# A divatos medve

Az Oroszország és az Egyesült Államok közötti kiber-hidegháború attól a pillanattól kezdve zajlik, hogy a hidegháború befejeződött, s míg az 1980-as évek végén a szovjet titkosszolgálatok a német hekkerektől kaptak titkos amerikai adatokat, néhány évvel később a feltörésekkel már maguk az oroszok kezdtek foglalkozni.

1996-ban a Moonlight Maze csoport, amely kapcsolatban állt az orosz hírszerzéssel, ellopta az amerikai kormányzat, valamint számos egyetem és más intézmény jelentős mennyiségű dokumentumát, beleértve a Pentagont és a NASA-t is. A támadás kivizsgálásába bekapcsolódott Robert Gourley, a tengerészeti titkosszolgálat tapasztalt munkatársa, aki a hidegháború idején a szovjet tengeralattjárókat üldözte. Amikor csapata a kiberkémek nyomát követte, kiderült, hogy a hekkereket érdekelte a hidrodinamika, az oceanográfia, a geofizika és a kémkedés technológiája is, hekkerkódjukban pedig cirill betűs töredékeket fedeztek fel.[227]

A támadásról szóló információk hamar megjelentek a sajtóban. A *Newsweek* hetilap *Kiberháborúban vagyunk* címmel közölt cikket.[228] A nyilvánosság először értesült arról, hogy az orosz hírszerzés többször is megkísérelte az amerikai technológiák megszerzését, de az amerikai védelmi minisztériumban azt közölték az újságírókkal, hogy „a kiberháború már a tetőfokán van". A katonai hivatalnokok a hekkereket „türelmesnek és állhatatosnak" nevezték, és azt feltételezték, az első behatolás után egyszerűen új eszközöket kezdtek bevetni: „Annyira mélyen hatoltak a hálózatokba, hogy jelenleg lehetetlen őket követni."

Végül is a Fehér Ház beleegyezett az FBI kérésébe, hogy ügynökei Oroszországban találkozhassanak az ottani hírszerzés képviselőivel. Az amerikaiak úgy döntöttek, nem úgy tárgyalnak a feltörésekről, mint az állam számára fontos ügyről, hanem egyszerűen segítséget kérnek az orosz kollégáktól a lopás kivizsgálásához. Moszkvába az amerikai hírszerzés körülbelül tíz munkatársa utazott el.

Úgy fogadták őket, mint kedves vendégeket: a látogatás teljes első napja egy kaviárral és vodkával folyó, szakadatlan pohárköszöntő volt. Másnap az amerikaiak az orosz védelmi minisztériumba mentek. Amikor a támadásokról kezdtek el beszélni, tárgyalópartnerük, a hadsereg tábornoka, zavartan a korcs felderítőket hibáztatta, és közölte, nem vesz részt hasonló cselekményekben. Ez volt az amerikaiak utolsó találkozója az orosz katonai vezetés képviselőivel: az FBI ügynökei még négy napot töltöttek Moszkvában, de a védelmi minisztériumba többet nem hívták őket. Az elkövetkező néhány évben az Oroszországgal kapcsolatban álló hekkerek nem hallattak magukról az USA-ban.

A londoni King's College professzora, Thomas Rid a következő két évtizedben folytatta a Moonlight Maze tevékenységének kutatását. 2016-ban a Moonlight Maze ügye abba az angol faluba vezette el őt, ahol az 1996-os támadásokat elemző számítógépes védelmi szakértő élt. Ridet az ő egyik számítógépe érdekelte, amelyet az orosz hekkerek törtek fel. A szakértő ezt mostanáig neki tartogatta. A londoni tudós a számítógépet a Kaspersky Lab szakértőivel megvizsgálta, és megtalálták a támadás idejéből származó kártékony kód egy részét. Kiderült, hogy ezt továbbra is használják az orosz államnak dolgozó hekkerek.

* * *

Az orosz hekkerek különböző amerikai intézmények elleni támadásai még évekig folytatódtak, de a legnagyobb visszhangot a 2015-ös feltörések váltották ki, és láthatóan ezek is voltak a leghatékonyabbak. Ekkor a Fancy Bear hekkerei



– akik úgyszólván megtestesítik az orosz kibersereget – az amerikai Demokrata Párt nemzeti bizottságának rendszerébe hatoltak be.

Ezt a lehető legegyszerűbb módon tették meg: phishing levelekkel (a CrowdStrike elemzőcég adatai szerint a demokratákat kétszer törték fel, 2015 nyarán és 2016 áprilisában). Miután megszerezték a hozzáférést a bizottság és a párt magas rangú munkatársainak levelezéséhez, az anyagot átadták a Wikileaksnek, amely a leveleket néhány hónappal az elnökválasztások előtt a nyilvánosság számára is elérhetővé tette. Ezekből a levelekből a demokrata elnökjelöltet, Hillary Clintont kompromittáló információk derültek ki: a pártkoordinátorok egymás között megtárgyalták, hogyan okozhatnának kellemetlenséget párton belüli konkurensének, Bernie Sandersnek, a párt egyik képviselője pedig előre egyeztette Clintonnal azokat a kérdéseket, amelyekre a nyilvános vitákon válaszolnia kellett.

A támadásért a felelősséget akkor a Guccifer 2.0 névre hallgató hekker vállalta magára. Álnevét a román Marcel Lazăr Leheltől kölcsönözte,* aki ekkor egy amerikai börtönben várta az ítéletet, amiért részt vett román és amerikai politikusok e-mail-fiókjainak feltörésében.

Guccifer 2.0 a weboldalán közölte, hogy Kelet-Európából származik, és meggyőződése, hogy a politikusok levelezését feltétlenül közzé kell tenni. A hekker külön kiemelte, hogy nem áll kapcsolatban Oroszországgal, és megjegyezte, hogy az összes későbbi hekkertámadás az oroszoknak tulajdonítható, annak ellenére, hogy ugyanezekkel a módszerekkel a világból bárhonnan lehet ily módon tevékenykedni. Guccifer 2.0 hangsúlyozta, hogy a mindenható orosz hekkerekről szóló mítoszt a Kaspersky Lab dobta be, saját üzleti érdekében.

Guccifer 2.0 tevékenységeinek, szavainak és fájljainak tanulmányozását száz ember vállalta annak érdekében,

* Az ő hekkerálneve volt Guccifer. – *A szerk.*

hogy a hekker vagy hekkerek orosz kapcsolatainak minél több bizonyítékát tárják fel. Az egyik leghasznosabb leletnek az ellopott levelek metaadatai bizonyultak: ezeket egy olyan számítógépen nyitották meg, amely az orosz nyelvet használja, az egyik levelet egy Feliksz Edmundovics nevű felhasználó kijavította:[229] a hekkerek látszólag ilyen formában hagytak üzenetet.

Amikor egyszer sikerült bejutnom az FSZB épületébe, rájöttem, hogy Feliksz Edmundovics Dzerzsinszkij* az orosz titkosszolgálat munkatársai számára változatlanul hősnek és szimbólumnak számít: a portréjával ellátott naptár ott lógott a lubjankai ház majdnem minden dolgozószobájában.

2016 júliusától az „orosz hekkerek" váltak az amerikai politika egyik legfőbb témájává. Clinton stábja azonnal azzal vádolta a Kremlt, hogy Donald Trump, a republikánus párti elnökjelölt támogatása érdekében szervezett támadást. Trump ezt tagadta, s később, amikor megnyerte a választást, továbbra is arról beszélt, hogy semmilyen formában nem működött együtt Oroszországgal, bár azt már nem zárta ki, hogy a hekkerek a Kreml megbízásából tevékenykedhettek. Vlagyimir Putyin sajtótitkára, Dmitrij Peszkov cáfolta,[230] hogy Oroszország bármilyen formában részt vett volna a támadásban.

Egyes amerikai hivatalok vizsgálatot indítottak a történtekkel kapcsolatban: 2017 januárjában az USA Nemzeti Hírszerzési Igazgatóságának Hivatala kiadott egy jelentést,[231] amely szerint Vlagyimir Putyin személyesen adott utasítást, hogy kezdjék meg „a beavatkozó kampányt" az amerikai elnökválasztásba. Erre a következtetésre az amerikai hírszerzés „szilárd meggyőződéssel" jutott.

***

* A szovjet belbiztonság, akkori nevén CSEKA, a KGB és az FSZB elődszervezetének megalapítója és első vezetője haláláig, 1926-ig.



A 2016-os támadások láthatóan egy orosz állami hírszerzési művelet részei voltak, ami már a 2000-es évek közepe óta zajlik. A Trend Micro nevű, kibervédelemre szakosodott szervezet rámutatott, hogy egy és ugyanazon csoport a 2000-es évek közepétől támadja azokat a szervezeteket és politikusokat, akik (orosz értelmezés szerint) fenyegetik Oroszország érdekeit. 2008-ban például megtámadták a Pentagont. A kibervédelemmel foglalkozó cégek az orosz hekkereket különféleképp hívják: hol Pawn Stormnak, hol APT28-nak, hol Tsar Teamnek, hol Fancy Bearnek, de ezek céljai nagyjából azonosak. A Fancy Bear például 2015 óta minimum négyezer-négyszáz phishing levelet küldött szét,[232] amelyek címzettjei között szerepeltek orosz ellenzékiek, számos európai ország politikusai, a NATO munkatársai és az amerikai Demokrata Párt. A hekkerek fertőzött csatolmányokat tartalmazó leveleket is küldtek.

A Nemzetközi Doppingellenes Ügynökség (WADA) 2016. szeptemberi feltöréséért a felelősséget legelőször a Fancy Bear vállalta magára. A csoport elindította a fancybear.net nevű weboldalát, ahol egy medve karikatúrája volt látható abban a jellegzetes maszkban, amely a hekkeraktivistákat tömörítő – a terroristák, a szcientológusok és a cenzúra ellen küzdő – Anonymous nevű mozgalom védjegye volt. Erre a weboldalra tették ki[233] a WADA dokumentumait. A feltörés néhány héttel azután történt, hogy eltiltották az orosz sportolókat a Rio de Janeiró-i olimpiától, mert tiltott szereket használtak. A dokumentumokból, amelyeket a Fancy Bear közölt, arra lehetett következtetni, hogy doppinggal – az ügynökség jóváhagyása mellett – ismert amerikai sportolók is éltek. A WADA képviselői a feltörésért Oroszországot vádolták.

A Fancy Bear és az orosz hatóságok közötti kapcsolatnak sokáig nem voltak közvetlen bizonyítékai. Arra, hogy ez a kapcsolat létezik, a szakértők szerint közvetett bizonyítékok mutattak:[234] például az a tény, hogy a hekkerek a moszkvai 9 és 17 óra közötti munkaidőben dolgoznak.

Az általuk használt kódban cirill betűs fragmentumok találhatók, a szerverek között oroszországiak is voltak,[235] az újságírók kérdéseire adott válaszokhoz pedig a hekkerek orosz VPN-t használtak. A fő bizonyíték mégis az maradt, hogy a támadásokat az orosz hatóságok érdekeinek megfelelően hajtják végre.

Az ESET nevű kibervédelmi szervezet szakértői elmondták, hogy a csoport „magas fokú műszaki támogatásával tűnik ki". Az ő adataik szerint a Fancy Bear folyamatosan használja „a nulladik napi sebezhetőséget", amely a programok korábban ismeretlen „réseit" jelenti (csak 2015-ben a Fancy Bear hat ilyenre talált rá a Windowsban, illetve a Java és Adobe Flashben; összehasonlításképp: a kiberharcos Stuxnet, amelyet az iráni atomprogram elleni támadásra alkalmaztak, négy nulladik napi sebezhetőséget használt fel).[236] A hasonló támadhatóságok, sebezhetőségek felkutatására alkalmas szakembereket a védelmi minisztérium különleges fejlesztési központjában gyűjtötték össze.[237]

Az ilyen „rések" felkutatása és kidolgozása bonyolult és hosszú munka, tehát komoly pénzügyi forrásokat is igényel. Emellett a csoport nem hajt végre[238] „kommersz támadásokat", mint amilyen a bankszámlákról lopás, és nem kereskedik saját kutatásai eredményeivel. (A nulladik napi sebezhetőségek ára a feketepiacon több tízezer dollárnál kezdődik.)

A Kaspersky Lab még 2014-ben nyilatkozott[239] az ART28 csoportosulásról, amely ugyanolyan módszerekkel tevékenykedik, mint a Fancy Bear: az amerikai választással kapcsolatos eseményekig a szakértők az állambarát hekkerekről jóval szabadabban beszélhettek. Az ART28 támadta meg a Fehér Házat és az amerikai külügyminisztériumot, phishing leveleket használva olyan videócsatolmányokkal, amelyek megnyitásakor a számítógépre letöltődtek a vírusok kiegészítő moduljai. A Kaspersky Lab, amely régóta követi a csoport tevékenységét, feltételezése szerint a kommentárok cirill betűs kódja miatt, valamint az operációs rendszerek verziója alapján, amelyeken írták a kódot, továbbá az időzónák miatt a csoport tagjai oroszok. Főként pedig azért, mert a feltörés módja, ahogy a feltörők használták, egybeesett más orosz nyelvű hekkercsoportokéival.



* * *

Az, hogy az amerikai Demokrata Párt szervereinek feltörése mögött nem pusztán orosz hekkerek állnak, hanem maga az orosz védelmi minisztérium és a GRU is, hivatalosan 2017-ben fogalmazódott meg abban a jelentésben, amelyet lényegében az Egyesült Államok összes hírszerzési szerve aláírt. Újabb másfél év elteltével részletek is napvilágot láttak: az amerikai esküdtszéki bíróság bizonyítottnak találta a vádat az orosz vezérkar tizenkét munkatársával szemben, akik a támadásokat végrehajtották. A bírósági dokumentumokban részletesen kifejtették,[240] hogy – az amerikai nyomozók verziója szerint – kik és hogyan lopták el az adatokat a demokratáktól.

A támadások többségét két épületből felügyelték: a Komszomolszkij sugárúton található 26 165-ös számú katonai részlegből (erről az épületről volt már szó korábban) és a Himka-toronyból, amelyet hivatalosan a „Hétköznapi tevékenységek igazgatási központjának" neveznek.

Az amerikai titkosszolgálatok dokumentumai szerint[241] Szergej Morgacsov alezredes vezényelte a katonai részlegnek azt az alosztályát, amely a hekkertevékenység informatikai hátterét kifejlesztette, beleértve az X-Agent programot is, amelyet kiváltképp gyakran használnak a kódtörők. Morgacsev munkáját négy hadnagy segítette. Borisz Antonov vezette azt a négyfős csoportot, amely phishing levelek révén feltörte a számítógépeket. Vele a GRU további három munkatársa dolgozott együtt.

Viktor Nyetisko (a GRU egyik vád alá helyezett munkatársa) a műszaki tudományok kandidátusa volt, 2003-ban védte meg a disszertációját *A számítógépek, a számítógépes rendszerek és hálózatok matematikai és programbiztonsága* szak-

területen. 2010-ben opponens volt az RGGU-n, az Orosz Állami Bölcsészettudományi Egyetemen egy disszertáció védésén, amely a számítógép-feltörésekről szólt. Az ő aláírása szerepel az akadémia és az FSZB, illetve egy sor moszkvai matematikai iskola közötti együttműködési szerződésen: ezek a dokumentumok arról tanúskodnak, hogy a tanulók készek belépni a védelmi minisztérium „tudományos századaiba". Volt még egy vádlott, Dmitrij Badin, aki 2014-ben részt vett a moszkvai *Positive Hack Days* című hekkerkonferencián.

A GRU munkatársai több mint háromszáz olyan számítógépet támadtak meg, amelyek kapcsolatban álltak az amerikai Demokrata Párt nemzeti bizottságával, a párt kongresszusi választásokat irányító bizottságával és Hillary Clinton elnöki kampányával. A leveleket a Google nevében küldték szét, mintha azok a biztonsági beállításokról szóló értesítést tartalmaznák. A leveleken belül pedig volt egy hivatkozás, amely arra a weboldalra vezetett, amit a GRU hozott létre.

2016 márciusában ily módon törték fel a Clinton választási stábját vezető John Podesta postaládáját. Postafiókjában több mint ötvenezer levél volt. Ezt követően a GRU munkatársai létrehoztak egy olyan postafiókot, amelynek a címe egyetlen betűben különbözött a Clinton-kampány egyik résztvevőjének címétől. Tőle küldték szét a phishing leveleket a stáb más kollégáinak. A levelek állítólag tartalmaztak egy hivatkozást a Clinton népszerűségi indexét tartalmazó Excel-dokumentumra, amely valójában a GRU által létrehozott weboldalra vezetett.

Ezzel egyidejűleg az orosz hírszerzés munkatársai megtámadták a Demokrata Párt nemzeti bizottságának a kongresszusi választásokkal kapcsolatos számítógépes rendszerét. A hozzáférést annak az adathalász levélnek a segítségével szerezték meg, amelyet a bizottság egyik munkatársnőjének küldtek. Ő végigment a neki küldött adatokon, és felvitte a jelszavát. 2016 áprilisától júniusáig



a vádlottak az X-Agent nevű kémprogramot legalább tíz számítógépre telepítették fel, olyanokra, amelyek csatlakoztak a pártbizottság hálózatához (ugyanezt a modult telepítették fel Ukrajnában abba a csatolmányba, amellyel a ballisztikai számítások programját támadták). A program rögzítette, milyen billentyűket nyomott le a felhasználó, felvételt készített a számítógép képernyőjéről, ezután pedig továbbította az ellopott adatokat arra a szerverre, amelyet a GRU bérelt Arizonában.

Az X-Agent segítségével többek között ellopták a kongresszusi választási bizottság tagjainak jelszavait, amely bizottságnak szintén volt hozzáférése a Demokrata Párt nemzeti bizottságának hálózatához. Nem kevesebb, mint harminchárom számítógépet törtek fel, amelyek ehhez a hálózathoz csatlakoztak.

A feltört számítógépeken a gyanúsítottak többek között olyan dokumentumokat kerestek, amelyekben említés történik Hillary Clintonra, Donald Trumpra, valamint a republikánus elnökjelölti küzdelem egy másik résztvevőjére, Ted Cruz szenátorra. Letöltöttek olyan fájlokat, amelyek a 2012-ben Bengáziban, az ottani amerikai konzulátus ellen végrehajtott terrortámadás következményeiről szóló információt tartalmazták (Hillary Clinton ebben az időszakban töltötte be a külügyminiszteri posztot, az üggyel kapcsolatban[242] vallomást tett az ezt vizsgáló kongresszusi bizottság meghallgatásán). Ezenkívül a hekkerek hozzáférést szereztek pénzügyi dokumentumokhoz is, többek között a Clinton-kampány adománygyűjtési terveiről.

Hogy terjeszteni tudják ezeket a dokumentumokat – az amerikai nyomozók verziója szerint –, a GRU munkatársai magukat a román hekkernek, Guccifer 2-nek adták ki. Amint azt a dokumentumok mutatják, 2016 júniusában, amikor Guccifer 2-t azzal vádolták, hogy ezzel a névvel csak az orosz titkosszolgálatok megbízottjait fedezi, a 74455-ös számú orosz katonai részleg szerveréről megkeresések érkeztek néhány angol mondattal kapcsolatban

(például az olyan szókapcsolatok fordítását illetően, hogy a „széles körben ismert fordítás" vagy az *illuminati* szó helyesírása). Valamivel több mint két óra múlva e mondatok mindegyike ott szerepelt Guccifer 2 közleményében, amelyben a „hekker" kategorikusan tagadta kapcsolatát Oroszországgal.

Ugyanekkor, 2016 júniusában, a vádlottak működésbe léptették a DCLeaks nevű weboldalukat, amelyre kiposztolták az ellopott levelek egy részét. Ezek terjesztéséhez fiókokat hoztak létre a Facebookon és más közösségi oldalakon. Ezenkívül az ellopott adatokat harmadik félnek továbbították, amelyet a vádiratban Organization 1-ként említenek: ennek kapcsán több mint valószínű, hogy a Wikileaksre gondolnak.

Azon néhány bizonyíték ellenére, amelyek alapján a GRU orosz hekkerei kapcsolatba hozhatók az amerikai választási kampány idején történt támadásokkal, a kérdések száma nem csökkent. Oroszország változatlanul tagadja, hogy köze lett volna a támadásokhoz, s egyik megnevezett GRU-munkatárs se kommentálta a vádakat. Egyik interjúalanyom – egy hekker, és az FSZB-nél dolgozott a nemzetközi hírszerzésen – a Moszkva külvárosában tett hosszú sétánk alkalmával azt mesélte, hogy még mindig kételkedik a GRU képességeiben. Ő maga biztos benne, hogy a támadásokat a fórumokhoz felfogadott hekker önkéntesek hajtották végre.

*31. fejezet*

## „Orkok" mint elvtársak

2016. december 5-én – mindössze egy hónappal Donald Trump elnökválasztási győzelme után – az orosz FSZB munkatársai megbeszélésre érkeztek kollégájukhoz, az Informatikai Védelmi Központ hivatalának egyik vezetőjéhez, Szergej Mihajlovhoz. Az értekezlet gyorsan véget ért: zsákot húztak Mihajlov fejére, és magukkal vitték. Ismerősei szerint a nyomozók tartottak attól, hogy Mihajlov – lévén fekete öves karatés – ellenállást tanúsít. Mihajlovot hamarosan a lefortovói börtönbe szállították, ahol jelenleg is fogva tartják.

Letartóztatása pillanatában a negyvenéves Szergej Mihajlov az Informatikai Védelmi Központ 2-es számú hivatalát vezette, ő felügyelte azokat a hekkereket, akik az FSZB-vel működnek együtt, valamint felügyelte azokat a feltöréseket, amelyek állambiztonsági érdekekhez kapcsolódtak. Gyakran utazott kibervédelmi témájú konferenciákra, ahol arról beszéltek, Oroszországban hogyan halásszák a kártyásokat.

Mihajlovot hazaárulással vádolták. Hamar kiderült, ez a vád azzal függ össze, hogy egy FSZB-munkatárs fedhette fel az amerikai titkosszolgálatok számára azoknak az orosz hírszerzőknek a nevét, akik az Egyesült Államok elleni hekkertámadásokat felügyelték. Már Mihajlov letartóztatása után írta a *The New York Times*,[243] hogy a hekkerek felkutatásában az amerikai titkosszolgálatok számára az Oroszországban található hírforrásaik bizonyultak a legfőbb segítségnek. Mihajlovnak volt hozzáférése ilyen adatokhoz, és az én forrásom azt mondta, az FSZB CIB 2-es

számú hivatala fejének sok fenntartása volt a GRU módszereivel kapcsolatban, úgy gondolta, „arcátlanul, durván és gorombán törik fel a szervereket", és a támadás nyomai „mindig láthatók".

Kis idő múlva kiderült, hogy nem Mihajlov volt az első, akit az FSZB munkatársai őrizetbe vettek az üggyel kapcsolatban. Mihajlov letartóztatása előtt egy nappal, 2016. december 4-én a Kaspersky Lab egyik topmenedzsere, Ruszlan Sztojanov kiment a moszkvai repülőtérre, hogy hivatalos útra repüljön Kínába. Miután becsekkolt a járatra, sms-t küldött a feleségének. A kínai vállalatnál, ahol várták, a következő napon nem jelent meg. Az utazás szervezői értesítették a Kaspersky Lab vezetését, hogy Sztojanov eltűnt. Néhány nap múlva a cég közölte, hogy megtalálták a kollégát a lefortovói börtönben, ahová az FSZB szállította.

Sztojanov hosszú éveken át foglalkozott kibervédelemmel: a 2000-es évek elején őrnagyi rangig vitte a belügyminisztérium „K" ügyosztályánál, és dolgozott az RTKomm.ru védelmi ügyosztályán is (a Rosztelekom leányvállalata 2016-ban a CIB FSZB-nek is szolgáltatásokat nyújtott). Aztán céget alapított, amely önálló kutatásokkal kezdett foglalkozni, 2012-ben pedig csatlakozott a Kaspersky Lab állományához, ahol a számítógépes incidensek vizsgálati osztályát vezette. „Ezt azon az ügyosztályon belül hozták létre, amely az FSZB-t és a belügyminisztériumot szolgálta ki – árulta el a társaság egykori, magas pozíciót betöltő munkatársa. – »Orkoknak« nevezték magukat, nagyon tetszett nekik ez az elnevezés."

Jevgenyij Kaszperszkij szavai szerint Sztojanov „igen hatékonyan dolgozott az FSZB Informatikai Védelmi Központjában". Az „orkok" kísérték a tettenérésre szakosodott csapatot, amikor azok őrizetbe vették a kiberbűnözőket. „Közvetlenül az FSZB-sekkel együtt utaztunk a megadott helyszínre, és Sztojanov nem restellt fényképes beszámolót is posztolni arról, hogyan fogták el például a Lurk csoportot" – emlékezett vissza a Kaspersky Lab egyik munkatársa.



Sztojanovot hazaárulás vádjával vették őrizetbe. Az volt a gyanú ellene, hogy ő továbbította az amerikaiaknak azt az információt, amit Mihajlovtól és Dmitrij Dokucsajevtől kapott, egy másik FSZB CIB-es munkatárstól, akit hasonló vádakkal illettek.

Dokucsajev, úgy tudni, az első olyan hekkerek egyike, akik állandó munkára mentek át a titkosszolgálatokhoz. A számítógépek iránt fiatalkora óta rajongott, és ezzel egy időben, mint oly sok kamasz, verseket írt. 2001-ben például ezeket a sorokat írta:

*Linux-Rules, Windows – örökké rossz*
*Ahogyan azt a barátaim mondták nekem*
*Eldöntöttem, hogy ellenőrzök, megvéve egy nulladik napi redhatot*
*Álomvilágban élni, lemezeket formázni.*
*De hirtelen valami érthetetlen van a képernyőn és a táblázatban:*
*Itt szükséges egy csere, itt meg egy tartalék lemez kell.*
*Nézem én a könyvet, lapozom minden oldalát...*
*Ekkor valaki ezt mondja: „üveg nélkül ne tedd meg"*
*Uff... Képbe kerültem... De a szektorok formázása már folyamatban*
*Ki kell választanom a komponenseket az installációhoz*
*Nem is tudom felfogni, a fejem ködben úszik*
*Minden ki van posztolva, de a Linux mindehhez kevés.*
*Eltelik egy újabb óra vagy kettő, hurrá, sikerült!*
*A beállítás megtörtént. Második próbálkozásra.*
*Izgulok, örülök, sírok a boldogságtól,*
*Nem, ez nem a RedHat, hanem egyszerűen kínszenvedés...*

Dokucsajev Kamenszk-Uralszkban született, amely egyórányi útra van Jekatyerinburgtól. Legutoljára Kamenszk-Uralszkban a 2013-as újévkor járt arra, azt követően, hogy ott megjelent[244] egy homoszexuálisokat üldöző radikális csoport (egy alkalommal kimentek egy férfival a temetőbe, és arra kényszerítették, ásson ki a földből egy

sírkövet, aztán pedig egy dzsipben megerőszakolták – az aktivisták az ilyen műveleteket „szafarinak" nevezték). Maga a hekker így írt a szülővárosáról: „Kétszázezer lakost számlál, ami nem is túl sok. Kamenszk-Uralszkban rengeteg gyár van, általában fémfeldolgozók – csövek, kohászat, alumínium. A város hamarosan háromszáz éves lesz. Nem is olyan öreg, de már nem is annyira fiatal. Nincs sok nevezetessége: ez természetesen nem Moszkva, de Kamenszkben van egy tájmúzeum, nagyon sok színház, könyvtár, stadion, sportkomplexum és internetkávézó."

Dokucsajev fiatalkorában az ideje nagy részét videójátékokkal töltötte, játszott a *Worms Armageddon*nal, a *Need for Speed*del, a *Quake* 3-vel. Az első feltörését a városi hálózat ellen követte el, hogy ingyenes hozzáférést szerezzen az internethez. „Mindig is azt gondoltam, hogy az információnak szabadnak kell lennie, ezért baromira nem szeretnék fizetni a szolgáltatóknak a hozzáférésért" – mesélte.[245]

A középiskola után Dokucsajev a jekatyerinburgi műszaki egyetemre jelentkezett, a technikai és technológiai információs rendszerek szakra, később rendszergazdaként dolgozott az egyik jekatyerinburgi egyetemi tanszéken. Részletesen mesélt magáról a saját weboldalán[246] (ez mostanra már nem elérhető), amelyet *Dmitry's homepage. The best...*-nek (Dmitrij honlapja. A legjobb...) nevezett. 2002-ben minden feszélyezettség nélkül azt írta, hogy „népszerűségre tesz szert az interneten, de nem csak. ☺ „A *Hekker* című folyóirat szerkesztőségével dolgozom együtt, és tűrhető honoráriumot kapok. ☺" Az álnevét – a Forbot – az angol *forbidden*, azaz tilos szóból képezte.

A lapban például *A hekker tíz végzetes tévedése* című anyaga jelent meg:

*A hekker első tévedése a szakmájának a megválasztása. Minden feltörés végzetes lehet a számára, és ezt a hekker jól tudja. De nem tud lenyugodni, mert a feltörést extrém sportnak tekinti. Ha még csak gondolkodsz azon, hogy „legyél vagy ne legyél hekker", akkor itt egy jó tanács: NE! Hekkernek lenni már nem annyira trendi,*



*ráadásul veszélyes is. Jobb, ha valami mással kezdesz el foglalkozni, például árulj orosz nyelvű szakdolgozatokat a neten. ☺ "*

Az általa fellelt sérülékenységek közzétételén kívül Dokucsajev a weboldalán saját magáról készült fotókat is megosztott: *Én a díványon* (1997*; kamasz, egy kockás flanelingben és tréningnadrágban ücsörög egy heverőn), valamint más fotókon a MIFI-n, a Krímben és a Fekete-tengernél egy diszkóban látható.

2004-ben Dokucsajev hitelkártyacsalással foglalkozott, és honlapokat tört fel megbízások alapján. Arról, hogy ezt hogyan csinálta, részletesen beszámolt a honlapján. Legfőbb érdemének az Egyesült Államok egyik kormányzati honlapjának a feltörését tartotta. 2006-ban Moszkvába költözött, és a *Hekker* című folyóirat munkatársaként kezdett dolgozni.[247]

Dokucsajev ismerősei szerint a költözést követően Dokucsajev feleségül vette a barátnőjét, akit hamar megtanított az orosz *Cosmopolitan* honlapjának a feltörésére. A hekker és a kollégái sokat buliztak és ittak együtt, időnként belekeveredtek egy-két balhéba. „A határtalanság még a kriminalitásig is eljutott, minden buli és találkozó féktelenül, de vidáman zajlott" – emlékezett vissza az egyikük. Az egyik esedékes ivászat alkalmával Dokucsajev három méter magasra ültette őt, hogy törje le egy térfigyelő kameráját. Ezután sikerült elmenekülniük a rendőrök elől, de beleütköztek az FSZB munkatársába, akitől a hekker „kapott egyet az állkapcsára".

Dokucsajev hamarosan az FSZB-vel kezdett együttműködni, majd állása is ott lett az FSZB CIB 2-es számú operatív hivatalának rangidős, mindenható műveleti szakemberekéként. Ez az ügyosztály az állam kibervédelmével és az ország biztonságára veszélyesnek számító hekkertámadá-

* *Én a díványon* (1997) lásd: https: //web.archive.org/web/20050421230800/http://kamensk.net.ru:80/forb/cgi-bin/foto.cgi?area=me&num=1

sok vizsgálatával foglalkozik. Dokucsajev 2016-ig dolgozott itt, amíg le nem tartóztatták.

Az egyik hekker, aki alkalmanként működik együtt a titkosszolgálatokkal, azt mesélte, hogy az FSZB szerint az USA azokat a hekkereket támadta meg, akiket a GRU felbérelt, nem pedig a hírszerzés állományban lévő munkatársait. Emellett meg van róla győződve, hogy Mihajlovot és Dokucsajevet már 2016 tavasza óta megfigyelték.

2018 áprilisában Dokucsajev alku keretében részleges beismerő vallomást tett, hogy adatokat továbbított külföldi titkosszolgálatok számára. Ám a vallomása nyilvánvalóan nem az állami hekkerekről, hanem a kártyásokról szóló adatok továbbításáról szólt. Szinte lehetetlen hitelt érdemlően megbizonyosodni arról, valóban a korábban a hekkereket felügyelő FSZB-munkatársak adtak-e át adatokat az amerikai titkosszolgálatoknak. A hazaárulással kapcsolatos bírósági tárgyalások mindig zártak az újságírók előtt. 2019. február végén Mihajlovot és Sztojanovot bűnösnek nyilvánították hazaárulás vádjában, és huszonkét, illetve tizennégy év börtönbüntetést szabtak ki rájuk. Hogy pontosan miből is állt össze a vád, valószínűleg örökre titok marad. Máskülönben Oroszországnak be kellene ismernie az USA elleni kibertámadás megszervezését.

*32. fejezet*

## Őszinte vallomás

Az egyetlen hekker, aki nyilvánosan elismerte, hogy támadásokat hajtott végre az Egyesült Államok ellen, Konsztantyin Kozlovszkij volt. Dmitrij Dokucsajev földije – ő is Kamenszk-Uralszkban született – és Ruszlan Sztojanov egykori „célpontja", Kozlovszkij volt az egyike azoknak, akiket a Lurk csoport tagjaként letartóztattak, miután orosz bankokat loptak meg.

2017. augusztus 14-én Kozlovszkij, aki ekkor már egy éve állt letartóztatásban a 2010-es évek legsikeresebb hekkercsoportjának létrehozása miatt, posztolni kezdett a Facebookon az FSZB-ben végzett munkájáról. Azt nem tudni, hogyan férhetett hozzá a közösségi hálóhoz a titkosszolgálatok ellenőrzése alatt álló lefortovói börtönben. Posztjaiban gyakran használta a #leleplezés, a #cyberwar, a #russianhacker, #USA_Demokraták és a #feltörés hashtageket, és kijelentette, hogy „igazságot" akar. „Nem hisznek nekem, hiszen nagyon megéri nekik, hogy meghurcoljanak a bíróságon bennünket azokért az összegekért, amelyek aztán bizonyos zsebekben landolnak – fejtegette. – A vallomásomra senki se kíváncsi, mivel nyilván sérti a nagy emberek terveit." A történtek Kozlovszkij-féle verziójának helyességét ellenőrizni ma már lehetetlen, állításai könnyen lehetnek a titkosszolgálati műveletek részei is.

Kozlovszkij ügyében a tárgyalás zárt ajtók mögött folyt, az újságírókat nem engedték be a tárgyalóterembe, de ismeretlenek a teljes tárgyalást felvették, és nyilvánosan elérhetővé tették.[248] Az első tárgyalási napon a hekker azt vallotta, sok éve dolgozik az államnak.

– Megtisztelő! Az FSZB-s tartótiszt Dmitrij Dokucsajev – közölte. – Ha egy mód van rá, idézzék be, kérem, a tárgyalóterembe. Szeretnék a szemébe nézni, mert sok ember van miatta őrizetben. Dokucsajev jelenleg fogoly, a lefortovói börtönben ül.

A bíróság megtagadta Dokucsajev beidézését. A következő tanúvallomásakor Kozlovszkij azt árulta el, hogy FSZB-ügynökök számára teljesített különböző feladatokat, beleértve az amerikai Demokrata Párt nemzeti bizottsága e-mailjeinek, illetve a Hillary Clinton és az amerikai hadiipari cégek közötti levelezés feltörését is.

„A teljes nyugati média a feltörésekről beszél. Én viszont azt akarom mondani, hogy ha valamiben bűnös vagyok, az csakis az, hogy ennek az államnak dolgoztam – közölte Kozlovszkij. – A többiek [a Lurk letartóztatott tagjai] semmiben sem vétkesek, egyik nap még csak gombokat nyomogattak, most pedig börtönben ülnek. Fáj a szívem amiatt, hogy kitettem őket ennek, és amiatt is, hogy az FSZB emberei így bánnak velünk."

Kozlovszkij szerint Dokucsajevvel és az FSZB-vel 2008-ban kezdett együttműködni, amikor ő tizenhat éves volt. Teljesítette tartótisztjei utasításait. A titkosszolgálatokhoz fűződő kapcsolatának történetéről részletesen beszámolt egy posztban, amelyet kitett saját Facebook-oldalára is:

*Számítógépes technológiákkal foglalkozom, emiatt nagyon sok netes fórumon voltam jelen. 2008-ban fogadtam 500 USA-dollárba, hogy meg tudom támadni a postai szolgáltatásokat, és egy e-mail példáján ezt be is mutattam. Az illető e-mail jelszavát nyilvánossá tettem a fórumon, és követeltem a pénzt a vitapartneremtől, és azt, hogy találkozzunk. A megbeszélt helyre két ember érkezett. Miután megállapították, hogy én vagyok, aki feltörte a postát, felmutatták az FSZB-igazolványukat, és követelték, hogy üljek be az autójukba. Mint később megtudtam, a Szverdlovszki körzet FSZB-hivatalának belső udvarára vittek* [Jekatyerinburg városába]. *Egy háromszor három méteres helyiségben töltöttem két napot. Enni nem adtak. Vizet*



*csak kétszer kaptam egy alumíniumtálban. A szükségleteim kielégítésére hoztak egy vödröt. Az FSZB munkatársai választás elé állítottak: vagy dolgozom velük, vagy börtönbe küldenek a postafiók feltöréséért. Beleegyeztem, aláírtam a dokumentumot.*

*Az együttműködés egy éve alatt rengeteg feladatot kellett teljesítenem. A kurátorom, Ilja* [aki később a bíróságon figyelmeztetett, hogy az FSZB-s Dmitrij Dokucsajevre figyeljek oda] *bízott meg feladatokkal, és ellenőrizte is azokat, továbbá ellátott a szükséges informatikai eszközökkel, valamint pártfogolt a jogvédő szervezetekkel kapcsolatos ügyekben.*

*Az utóbbi években a fókuszunkba az amerikai és az EU-s szerverek kerültek. Az USA Demokrata Pártja nemzeti bizottságának és Hillary Clinton levelezésének feltörésére szóló megbízatásokat sikeresen teljesítettem, majd egy merevlemezen továbbítottam az adatokat Iljának, az FSZB munkatársának (850 gigabájt anyagot tömörített formában a feltörés videófelvételeivel).*

Kozlovszkij a támadásokat a titkosszolgálatok terminusát használva „megbízásoknak" nevezte. Az Egyesült Államokra és az Európai Unió országaira irányuló „megbízások" célja az volt, hogy megszerezzék a hozzáférést a legnagyobb ipari vállalatok, állami és a katonai szervezetek, pénzintézetek (bankok, tőzsdék), sportszervezetek (FIFA, NOB, WADA), atomerőművek, vízierőművek, illetve az elektromos művek számítógépes hálózataihoz, valamint a legnagyobb hírmédiumok és azok közösségimédia-fiókjához" – írta. Kozlovszkij azt mesélte, hogy „egyszer az FSZB megbízásából posztoltam egy bejegyzést Mihail Sz. Gorbacsov haláláról a *RIA Novosztyi* mikroblogjára." Ez valóban megtörtént, 2013. augusztus 8-án.[249] Azt is megerősítette Kozlovszkij, hogy az FSZB utasítására szerezte meg a 2014-ben Donyecktől nem messze lelőtt Boeing-gép katasztrófáját kivizsgáló nyomozók személyes adatait és törte fel a számítógépeiket is.

Egy alkalommal, Kozlovszkij elmondása szerint, a titkosszolgálatok azt követelték tőle, hogy hozzon létre egy

„vörös gombot": ez a műszaki megoldás lehetővé teszi, hogy összpontosítva tegyék tönkre a kritikus infrastruktúrákat – gyárakat, atomerőműveket, tőzsdét – az Egyesült Államokban és Európában. Kozlovszkij ezt visszautasította, mert elhatározta, „nem akarja, hogy köze legyen a harmadik világháború kitöréséhez". Kis idő múlva ismét utasították ugyanerre, amit ő ismét hárított, mire azt a választ kapta: „A visszautasítás kedvezően nem végződhet." Ezt követően az őt felügyelő FSZB-ügynök eltűnt. Kozlovszkijt hamarosan őrizetbe vették, és a Nemzeti Gárda repülőgépével Moszkvába szállították. A számítógépeket és más tárgyi bizonyítékokat, amelyek alátámasztják Kozlovszkij verzióját, a hatóságok lefoglalták.

2017 áprilisában Kozlovszkij levelet írt az FSZB igazgatójának, Alekszandr Bortnyikovnak, amelyben közölte, „azt hitte, az állam érdekeiért cselekszik", és csak azért kényszerült elhíresztelni részvételét a külföldi országok elleni támadásokban, mert a vizsgálat során életfogytiglani börtönnel fenyegették.

A titkosszolgálatokkal együttműködő hekkerek azt mondják, a legtöbb művelet hasonlít azokhoz, amelyekről Kozlovszkij beszél, de ezeket nem tudják egyedül végrehajtani, Kozlovszkij története csak részben tűnik reálisnak, és a toborzást szolgálja. „Általában az ilyen infrastruktúrákon egész kiberhadseregek és osztályok dolgoznak, amelyeknek meg kell találniuk a védelemben a nulladik napi sérülékenységeket, különösen a jól védett katonai és más kritikus objektumokban" – fejtegeti az egyik toborzott hekker. Egy másik arra mutatott rá, hogy a nemzetközi kiberműveletekkel a GRU foglalkozik, az FSZB felelősségi köre az orosz belügyekre terjed ki.

Dokucsajev kijelentette, hogy nem ismeri Kozlovszkijt, és visszautasította a vádakat. A Kozlovszkij családnév nem szerepelt egyik hivatalos amerikai vizsgálati anyagban sem.

Végeredményben eddig senki nem állt elő cáfolhatatlan bizonyítékokkal arra nézve, hogy az amerikai politikusokat orosz hekkerek törték fel, ahogyan arra sem, hogy ezek az emberek kapcsolatban álltak a Kremllel. „Nincsenek használható műszaki naplóbejegyzések. Egyesek szerint a feltörések abban az időzónában történtek, amely a moszkvaival azonos. Nos, motivációnak is lennie kéne. De még a motiváció sem bizonyíték – világított rá az egyik kibervédelmi konferencián Veszta Matvejeva bűnügyi szakértő a Group-IB nevű társaságtól, amely Oroszországban a kiberbűncselekmények felderítésével foglalkozik, gyakran a titkosszolgálatokkal karöltve. – Azt is mondják, hogy a szerver Oroszországban található. De melyik normális hekker fogja megtámadni a saját számítógépéről az amerikai választásokat? A kódban található orosz nyelvű sorok szintén nem igazán számítanak bizonyítéknak. Amint az a tudomásunkra jutott, az észak-koreai hekkercsoport, a Lazarus a kódban orosz szavakat használ, hogy összezavarja a nyomokat – *nachalo, vykhodit, poluchit, derzhat* és így tovább. Be lehet vajon bizonyítani, hogy ez mégis orosz? Be. Mindig el lehet jutni konkrét személyekig, de a politika ezt most megakadályozza. Ha az egész világ nyomozni kezd, és minden ország rendelkezésre bocsátja a szerverei és a VPN-jei adatait, majd akkor lesz eredmény.

*33. fejezet*

## Az én számítógépes védelmem

Mint minden háborúban, a kiberkonfliktusok esetében ugyanúgy fontos a védelem is, nem csak a támadás. Egészen a közelmúltig az orosz állam gyakorlatilag nem beszélt az állami weboldalak és a kritikus infrastruktúrák – az atomerőművek, a haditermelést végző gyárak, a közellátási rendszerek és más objektumok – védelmének a feltétlen szükségességéről, holott az ezek elleni sikeres támadások gazdasági vagy pénzügyi katasztrófát okozhatnak, sőt emberáldozatokkal járhatnak. Az utóbbi években megváltozott a hozzáállás, valószínűleg elsősorban a létfontosságú objektumokba történő hekkerbehatolásokról szóló hírek miatt (például egy amerikai atomerőmű ellen történt ilyen támadás).[250] A terrorista szervezetek is fejlődtek a kiberkémkedés terén, tevékenységük egyre nagyobb mértékben jelent kiberfenyegetést.

„Azt gondolom, a kiberfegyverkezés tiltásáról szóló dokumentumot hamarosan alá fogják írni – jegyezte meg egy interjúban nekem annak a társaságnak az egyik munkatársa, amely a kritikus állami infrastruktúrák védelmével foglalkozik. – De majd ha csak valami nagy katasztrófa történik." Habár a NotPetya nevű vírus e beszélgetés után támadott meg számítógépeket világszerte, mégsem jelent meg semmiféle nemzetközi iniciatíva a kiberfegyverkezés korlátozására.

Interjúalanyom, aki a kritikus infrastruktúrák informatikai védelmével foglalkozik, azt mondja, a stratégiailag fontos orosz objektumok gyakran „feleslegesnek" találják a támadásokra való felkészülést. „Tárgyalunk velük, milyen problémák vannak a rendszereikkel, de nem ismerik



be, hogy náluk valami nem megfelelően működik. Azt mondják: ez csak egy egyszerű vírus, csak pénzt akar lopni – meséli. – De hiszen zárt infrastruktúrában tűnt fel! És nekik még szerencséjük van, hogy az a vírus csak erre képes. De mi lett volna, ha más a feladata?"

A jogvédő szervezetek és a velük jogviszonyban álló cégek időről időre beszélnek ugyan az orosz állam elleni kibertámadásokról, de nyilván jóval ritkábban, mint hogy azok valójában bekövetkeznének. Például 2013-ban Oroszország ellen a Sputnik vetett be kiberfegyvert (erről csak az Echelon, a globális megfigyelőrendszer által végzett kutatások alapján vannak ismereteink.[251] A rendszer külföldi szoftverek hatósági tanúsítványainak igazolásával foglalkozik a védelmi minisztérium megbízásából). A program célja kiberkémkedés volt, azaz információt gyűjtött a honvédelmi feladatokat ellátó intézmények, intézetek, diplomáciai szervezetek tevékenységéről, kihasználva egy rést Word-, Excel-, Outlook- és Windows-csatolmányokban. Hogy hová kerültek az ellopott információk, nem sikerült megtudni: a rendeltetési helyet elrejtette a proxyszerverek* láncolata. Az Eselon munkatársai szerint az ellopott információk Oroszország geopolitikai ellenfeleit érdekelhetik, és arra következtettek, hogy „a kiberháború, mint az államok közötti szembenállás formája, aktivizálódott".

2016 júliusában az FSZB közölte,[252] hogy trójaiakat észlelt az ország kormányzati, tudományos és védelmi hivatalai informatikai infrastruktúrájában (összesen körülbelül húsz szervezetnél). Az FSZB rámutatott, hogy a támadást pontosan megtervezték és profi módon valósították meg. Minden szervezethez saját exploitot[253] írtak, az áldozatokat phishing levelekkel fertőzték meg. A fertőzés után a programba feltöltötték a szükséges modulokat, amelyek lehetővé tették, hogy bekapcsolják a webkamerákat és mikrofonokat, megszakítsák a hálózati forgalmat, és lementsék

* Lásd *Fogalomtár.*

azokat az adatokat, amelyeket a felhasználók a billentyűzeten begépeltek. A parlament védelmi bizottságában ekkor hangzott el,[254] hogy az ehhez hasonló kiberkémkedés „mindenekelőtt az amerikaiaknak kedvez".

Adathalászattal a kínai állambarát hekkerek évek óta támadják[255] az orosz hadi intézményeket. „Egy konkrét csoport már 2008 óta dolgozik ezen – mutattak rá beszámolójukban a Positive Technologies szakemberei. – Az orosz védelmi minisztérium tisztjeinek postafiókjához megszerzik a hozzáférést, és beindítják a kártékony csatolmányok szétküldését." A levelekben arról volt szó, hogy a katonai szolgálatot teljesítők többet kapnak", és hogy „megemelik a katonai szolgálatot teljesítők fizetését". A fertőzés után a hekkerek követni tudták a fertőzött számítógépeket, letöltötték onnan az információkat, felvételt készítettek a képernyőről, aktiválták a mikrofont és a webkamerát. Az ilyesfajta feltörések nem pusztán a titkos dokumentumok kiszivárgásához vezettek, hanem hozzáférést adtak a hekkerek számára a kritikus infrastruktúrához is, hogy ezt aztán felhasználhassák komoly provokációkhoz, és akár kiberháború megkezdéséhez is.

Jelenleg az interneten folytatott érintkezéseik védelmére az orosz hivatalnokok a zárt állami hálózatot, az RSNet-et használják.[256] Minden munkatársnak van egy védett dolgozói postafiókja, ahová csak egy meghatározott IP-vel és számítógéppel lehet belépni, de messze nem mindenki tartja be a szükséges előírásokat, különösen a hatalom legmagasabb fokán. Fontolóra kellene venni a telefonbeszélgetések védelmét is: a titkosszolgálatoknak dolgozó egyik kutatóintézet 2017-ben forgalomba hozta[257] a „kriptotelefont", amely a hívások titkosítását teszi lehetővé.

* * *

Az amerikai Nemzetbiztonsági Ügynökség orosz megfelelője, a FAPSZI az 1990-es évek elején jött létre.[258] A hivatalt a szovjet KGB 8-as számú hivatala alapján hozták létre,



amely többek között a kormányzati kapcsolatokért és a hatalom legmagasabb szintjei által használt titkosított információkért felelt (itt dolgozott és sakkozott a barátaival a 28. fejezetben emlegetett Mihail Maszlennyikov). A FAPSZI egyik vezetője, Vlagyimir Markomenko az állami dumában elhangzott felszólalásában, 1996-ban, kijelentette,[259] hogy az USA titkosszolgálatai folyamatosan erőszakosan igyekeznek megszerezni más országok, így Oroszország informatikai és telekommunikációs komplexumainak anyagait. Kertelés nélkül rámutatott arra, hogy az orosz állami szervek hanyagul viszonyulnak az informatikai biztonsághoz.

Markomenko úgy vélte, a világban régóta folyik az „információs háború", és Oroszország ezt nem hagyhatja figyelmen kívül. „A hadműveleteket" ebben a háborúban egy tisztviselő csak így képzelheti el: „az ellenség védelmi rendszerének, informatikai és telekommunikációs rendszerének, infrastruktúrájának nyomás alatt tartása", az „információk megkaparintása", „az ellenség informatikai erőforrásainak feltörése", „harc a közvéleményért dezinformációk terjesztésével az ellenség információs csatornáin és a globális hálózatokon keresztül, valamint tendenciózus információk terjesztése értékítéletük befolyásolása érdekében, továbbá a lakosság és a döntéshozók dezorientálása". Mindez később valósággá vált.

A FAPSZI munkájának hatékonyságát nehéz értékelni. A hivatal egyik munkatársa azt mondta,[260] miközben adminisztrátorként dolgozott egy számítógépes klubban, kétszer annyit keresett, mégis elment szolgálni az államot, hogy „igazolványt" és „némi cselekvési szabadságot" kapjon: „Ott lehet kevesebb feltörést végezni, és természetesen a kis kétes üzelmek felett is szemet lehet hunyni." A FAPSZI-t 2003-ban feloszlatták, az alosztály egy része az FSZB állományához, más része az FSZO-hoz, a Szövetségi Biztonsági Szolgálathoz ment át.

* * *

Kibervédelmi szakértők évekig arra próbálták felhívni a figyelmet, hogy a hekkerek meg fogják találni a módját, hogy valódi fizikai kárt okozzanak a kritikus objektumoknak. 2009-ben ez meg is történt, amikor Irán ellen bevetették a Stuxnetet, azt a kiberfegyverzetet, amelyet speciálisan arra dolgoztak ki, hogy megzavarja az iszlám köztársaság atomprogramját. Ahogyan azt a *The New York Times* újságírója, David E. Sanger írta,[261] a Stuxnet létrehozásának célja az volt, hogy békésen oldják meg a problémákat: az Egyesült Államok attól tartott, hogy Izrael bombázni kezdi Iránt és annak atomerőműveit.

A hírforrások rámutattak,[262] hogy a Stuxnetet együttműködésben hozta létre több ország titkosszolgálata: az amerikai CIA és NSA, valamint az USA kibernetikai parancsnoksága, Nagy-Britannia kommunikációs figyelőszolgálata (GCHQ) és az izraeli Moszad rádióelektronikai hírszerzésének speciális alosztálya. A terveik megvalósításához a titkosszolgálatok először öt iráni társaságot támadtak meg,[263] amelyek kapcsolatban álltak az urándúsítással foglalkozó gyárral. Ezt követően a Stuxnet felkerült a munkatársak pendrive-jára, ők pedig, erről mit sem tudva, megfertőzték a gyár védelmi hálózatát, amely nem volt csatlakoztatva az internethez. Amikor az atomenergetikával kapcsolatban álló szervezetek irányítási rendszerének megtámadására kifejlesztett Stuxnet bekerült az iráni Natanzban lévő urándúsító gyár rendszerébe, megsemmisítette a centrifugáinak több mint negyedét úgy, hogy egy rosszindulatú kódot juttatott be a programba, amely megváltoztatta a berendezések viselkedését.

A centrifugák egy elektromos motor segítségével jöttek működésbe, másodpercenkénti ezres fordulatszámmal forogtak. A Stuxnet ezt a sebességet ezernégyszázra növelte, aztán pedig drasztikusan lejjebb vette, aminek eredményeképp a centrifugák tönkrementek. A gyár mérnökei, akik a szomszéd helyiségben tartózkodtak, azt látták a



képernyőjükön, hogy minden folyamat normálisan zajlik. Sokáig nem értették, mi volt a balesetek oka: néhányukat elbocsátották, azzal vádolva őket, hogy megsértették az üzemeltetés szabályait.

A támadások után a Stuxnet elterjedt más országokban is: 2010-ben világszerte körülbelül százezer számítógépet fertőzött meg, behatolt az egyik orosz atomerőmű rendszerébe is. Ahogy az iráni gyárak, úgy ez az atomerőmű sem kapcsolódott az internethez. Az egyik megfertőzött erőmű komoly biztonsági problémákra világított rá.

Azóta a kiberfegyverkezés új fajtái jelentek meg, amelyek hasonló módon működnek. 2016-ban az ESET szakemberei közölték, hogy megjelent az Industroyer nevű program, amelynek célja, hogy beleavatkozzon az energetikai társaságok irányítási rendszerének kritikus folyamataiba: ily módon a hekkerek képesek irányítani a kapcsolókat az alállomásokon. „Az Industroyer képessége hatással van az ipari berendezések munkájára, és idővel jóval veszélyesebb fenyegetést jelent a Stuxnetnél" – közölte a társaság. A szakértők feltételezik, hogy az Industroyer lehetett az oka a kijevi áramszünetnek 2016 decemberében. A világítás a város négy kerületében szűnt meg.

2017. június 23-án a *The Washington Post* azt közölte,[264] hogy Barack Obama, még elnöksége alatt* megbízta a Nemzetbiztonsági Ügynökséget egy Oroszország elleni kiberfegyverzet kifejlesztésére, válaszul arra, hogy az oroszok feltehetően beavatkoztak az amerikai választásokba. A speciális művelet célja volt olyan „implantátumokat elhelyezni" az orosz elektromos infrastruktúrába, amelyek a megfelelő pillanatban aktiválhatók. Az újságírók ezt „a bomba internetes analógiájának" nevezték. Az amerikaiak nem ekkor használták először ezt a technológiát: az NSA és a CIA egykori igazgatója, Michael Hayden azt mondta,[265]

* Barack Obama 2017. január 20-ig volt hivatalban.

hogy az Egyesült Államok a 2010-es években is helyezett el „implantátumokat", mégpedig tízezer számítógépen világszerte, „amelyeket majd fel lehet használni, amikor arra szükség lesz".

* * *

Még az 1990-es évek végén csecsen terroristák hajtottak végre támadást[266] orosz állami erőforrások és tömegmédiumok ellen. 1999. december 13-án feltörték az ITAR-TASZSZ hírügynökség főoldalát, pár hónappal később pedig az RBK* főoldalán helyeztek el fenyegető szöveget az oroszoknak és Vlagyimir Putyin elnök megbízottjainak címezve.**

Csaknem húsz év elteltével a kibertámadások továbbra is a radikális csoportosulások tevékenységének részei maradtak, de ma már sokkal komolyabb fenyegetésekről van szó, mint egyszerűen honlapok feltöréséről. „Mivel Oroszország részt vett a közel-keleti hadműveletekben, fölöttébb idegesíti a terroristákat – jelentette ki egy védelmi konferencián, 2017. június 30-án Ilja Szacskov, az informatikai védelemmel foglalkozó Group-IB nevű társaság munkatársa. – Mi, sajnos, már ebben az évben is beleütköztünk a kritikus infrastruktúra elleni sikeres támadásba." (Nagyjából Szacskov beszédének ideje alatt történt a történelem addigi legnagyobb hekkertámadása, a NotPetya vírus elterjesztése – erről részletesebben a 35. fejezet szól).

Egy évvel azután, hogy az Iszlám Állam vezetője kihirdette a kalifátus létrehozását Szíria és Irak területén, a terrorista szervezet kifelé irányuló propagandája erősen megváltozott: azon posztok és videók helyett, amelyekben újoncok agitáltak az Iszlám Állam oldalán folytatott harcra, olyan anyagok kezdtek megjelenni, amelyek az új állam felépítéséhez nyújtott segítségre buzdítanak, ami orvosokat, tanárokat, újságírókat, programozókat igényelt. Nagyjából ugyanekkor az Iszlám Államban is megjelent egy hekkeralosztály, az ISIS Hacking Division264,[267] más néven a Kiberkalifátus. Ezt a nagy-britanniai Birminghamből átköltözött hekker, Trick (TriCk) szervezte meg.

Tricknek ekkorra már nagy tapasztalata volt: első feltörését tizenegy évesen követte el,[268] hogy bosszút álljon riválisán egy online játékban, tizenöt évesen pedig létrehozta a *Team Poison* nevű hekkercsoportot. Ennek nem pénzkereset volt a célja, hanem az ellenállás: Trick feltétlenül szükségesnek vélte a harcot a palesztinok és a Kasmírban élők jogaiért. E harc részeként támadta meg társaival együtt az Izrael-barát és amerikai médiát, illetve a közösségi felületeket, s például saját jelmondatokat és figyelmeztetéseket helyezett el az ideológiailag ellenséges honlapok főoldalain.

A Team Poison megtámadta a NATO weboldalait, a brit védelmi minisztériumot és Mark Zuckerberg Facebook-fiókját. 2012-ben, miután feltörte az egykori brit miniszterelnök, Tony Blair tanácsadójának e-mailjét,[269] Tricket megtalálták és letartóztatták. A hekkerről kiderült, hogy a neve Junaid Husszain, pakisztáni emigránsok fia. Fél évet egy angol börtönben töltött, szabadulása után az Iszlám Állam fővárosába, Rakkába utazott, ahol felvette az Abu Huszszain al-Britani nevet és a szervezet vezető hekkerévé vált.

Ebben a minőségében azt a tevékenységet folytatta, amihez a leginkább értett: amerikai weboldalakat és közösségi oldalakat tört fel. Például[270] 2015 januárjában ő helyezte el az amerikai központi katonai parancsnokság Twitter-oldalán az „USA katonái, jövünk, vigyázzatok magatokra" posztot. A hekker felfedte az amerikai katonák személyazonosságát és lakcímét is, felszólítván híveit, hogy találják meg és öljék meg őket. 2015 nyarán Trick két Iszlám Állam ellen küzdő aktivista személyét is leleplezte, őket ki is végezték. 2015. augusztus elejétől a huszonegy éves Husszain harmadik helyen szerepelt a Pentagon által likvi-

* Az RBK az egyik legnagyobb orosz médiavállalat nevének a rövidítése. A vállalathoz tartozik egy tévécsatorna, egy hírügynökség, egy újság és egy folyóirat is. – *A ford.*

** Vlagyimir Putyin valójában 1999. december 31-ig miniszterelnök volt, Borisz Jelcin elnöksége alatt. – *A szerk.*

dálandóként számontartottak listáján,[271] a kalifátust vezető Abu-Bakr al-Bagdadi és az Iszlám Állam hóhéra, a magát Dzsihád Johnnak nevező férfi mögött.

Néhány nappal ezután egy fedett ügynök kapcsolatba lépett a hekkerrel a *Surespot* nevű védett messengeren keresztül (Trick kiposztolta a kontaktjait a Twitteren, hogy tudjanak levelezni vele az elvrokonai.) A chat alatt az illető egy olyan oldal linkjére csalta fel Husszaint, amelyről a hekker telefonját vírussal támadta meg. Ezután követni tudták őt, míg végül dróntámadás során Husszaint likvidálták. A fedett ügynök nem más volt, mint a hekker Shm00p, aki Trick halála után ezt írta:[272] „Én, basszus, bűnös vagyok, sajnálom, egy játékot játszottam, amelyet nem kellett volna [játszani]." Azt hangoztatta,[273] hogy azért segített a titkosszolgálatoknak, mert azok megfenyegették a családját, és azt állította, hogy becsapták. „Segítettem önöknek MEGÖLNI őt. Mit gondolnak, most tudok éjszaka aludni? – írta Shm00p. – Ő terrorista volt és egy állat, de úgy érzem, engem elárultak."

Husszain likvidálása ellenére a kibervédelem szakemberei hamarosan szerte a világon észlelni kezdték, hogy az alvilági fórumokon növekszik a terrorista csoportosulások érdeklődése a hekkertámadások iránt, különösen azok iránt, amelyek a kritikus infrastruktúrák ellen irányulnak. Erről az egyik interjúalanyom beszélt, aki a hekkerek kommunikációs platformjait vizsgálta. Információját a Group-IB egyik beszámolója is megerősíti.[274] Az orosz titkosszolgálatok egyik ügynökétől megtudtam, hogy szíriai IP-című felhasználók kiberbiztonsági szakembereknek ajánlanak munkát, és érdeklődést mutatnak a kiberháború folytatásának módszerei iránt. A fórumokra írt üzeneteiket alapvetően a Google Translate segítségével írják. A terroristák az iránt is érdeklődnek, hogy miként lehet behatolni a védelmi cégek rendszerébe, hogy ellophassák titkos fejlesztéseiket. Amint arról a *The New York Times Magazine* beszámolt, a különböző hekkercsoportok már hosszú évek



óta keresik[275] a „vörös higanyt", a Szovjetunió által kidolgozott harcászati fejlesztést, amelyet állítólag fel lehet használni egy tömegpusztító fegyver létrehozásához.

„Ha az Iszlám Állam hívei rájönnek, hol tudnak hozzájutni pénzért a nulladik napi támadhatóságokhoz, akkor nem a legjobb eseményeknek nézünk elébe" – mondja egy a kritikus infrastruktúrával foglalkozó biztonsági szakember. „Az emberiség a terrorizmussal a 19. század óta harcol – fejtegeti az információs védelem szakembere, Ilja Szacskov. – A kibertér védelméről szóló tudomány nagyjából húsz évvel ezelőtt született meg, de komolyan terrorizmussal az interneten soha korábban nem találkoztunk. Csak pontszerű támadásokkal – mint amilyenek Ukrajnában vannak."

* * *

A Stuxnet sikere az iráni atomprogram ellen folytatott harcban nem maradt észrevétlen Oroszországban sem. 2013 januárjában Vlagyimir Putyin megbízta az FSZB-t,[276] hogy hozza létre a számítógépes támadások következményeit feltáró, az azokra előre figyelmeztető és a következményeket feltáró állami rendszert (a GoszSZOPKA-t). A terv az volt, hogy „fedjék be" az összes állami információs forrást egyetlen rendszer „búrájával", amely folyamatosan monitorozza a teljes területet, így figyelemmel kísérhető az összes, internetről érkező információ. Elhatározták, hogy ehhez a rendszerhez hozzákapcsolják a kritikus infrastruktúra összes erőforrását és objektumát, hogy azok információkat tudjanak cserélni a támadásokról a legfőbb centrumon keresztül. Ennek a centrumnak kellett megállapítania, hogyan épül fel a támadás, és ajánlásokat kellett küldenie a GoszSZOPKA egyéb résztvevőinek a védelemről.

A rendszer koncepcióját két év alatt hagyták jóvá. 2015-ben az FSZB közölt[277] egy erről szóló kivonatot. Ott rámutattak, hogy a GoszSZOPKA-t reagáló alközpontokra osztják fel az egyes régiók és hivatalok szerint, és hogy az FSZB

mellett létrehozzák a számítógépes incidensekre szakosodott Nemzeti Koordinációs Centrumot (a Gov-CERT-et), amely a kritikus infrastruktúra védelmével foglalkozik majd. A Gov-CERT-et az FSZB munkatársa, Alekszej Novikov vezette; közlése szerint 2016 novemberétől a rendszerhez tíz állami szervet kapcsoltak, és a hatósági reagálóközpontokat már a Centrobank (az orosz központi bank) és a Rosztech is működésbe léptette.[278]

Novikov kifejtette,[279] hogy a titkosszolgálatok most építik ki behatolásokról szóló információcsere támogatását az állami szervek között. Ahogy elmondta, a rendszerben különleges rend érvényesül: az illetéktelen behatolásokról szóló információt eljuttatják a központba „az együttműködés teljesítésére vonatkozó kéréssel" együtt. Az ilyen információk elsőbbséget élveznek minden más információval szemben, a Nemzeti Koordinációs Centrum ügyeletes műszakja pedig ezekről az incidensekről azonnal lát mindent és cselekedni kezd: például az internetszolgáltatókon keresztül átszűri a kártékony információáramlást, vagy megpróbálja megszüntetni a botnetek működését. A hivatalnok megerősítette, hogy még 2014-ben a szocsi olimpia ideje alatt az FSZB-nek sikerült kivezetnie a rendszerből néhány botnettel irányított központot.

Ezenkívül az FSZB felhívta mindenkinek a figyelmét, hogy a köztisztviselők körültekintően bánjanak az elektronikus leveleikkel. „Az egyik állami testület (gyanús) leveleket kapott, a biztonsági szolgálat munkatársai átküldték őket vizsgálatra hozzánk – emlékezett vissza Novikov a 2017. februári Urál fórumon.* Lefuttattunk egy gyors analízist, és egy ismert (vírus)családot tártunk fel. Azt is meg tudtuk állapítani, honnan küldték a leveleket. Kiderült, hogy addigra azok már tíz objektumba eljutottak, de a további támadásokat el tudtuk hárítani."

* Évente megrendezett konferencia a pénzügyi szektor informatikai biztonságáról. – *A szerk.*



2016 decemberében Dmitrij Medvegyev miniszterelnök az állami duma elé terjesztette a kritikus informatikai infrastruktúra védelméről szóló törvénytervezetet, amely minden objektumot kötelez az információcserére a GoszSZOPKA-val. A dokumentum nemcsak egy különleges, a számítógépes rendszerek listájának elkészítését írja elő, amelyeket a kritikusan fontos objektumokban használhatnak, de kilátásba helyez egy új büntetőjogi cikkelyt is kritikus informatikai infrastruktúra elleni támadás esetén. Az emiatt kiszabható maximális büntetés tíz év börtön; egyébként ezt a büntetést nemcsak hekkerek kaphatják, de azok az állami szolgálatot végzők is, akiknek az elnéző magatartása miatt a kiszivárogtatás vagy a támadás bekövetkezhetett.

A törvénytervezetet felülvizsgáló FSZB véleménye szerint, ha nem tesznek mielőbbi lépéseket az informatikai infrastruktúrák védelme érdekében, a terroristák és a külföldi titkosszolgálatok az ország stabilitását fenyegetik: Oroszország „közvetlenül függ az informatikai és telekommunikációs hálózatok és az informatikai rendszerek biztonságos működésétől". „A legrosszabb forgatókönyv szerint egy számítógépes támadás képes teljesen megbénítani az állam kritikus informatikai infrastruktúráját, és szociális, pénzügyi és/vagy ökológiai katasztrófát is kiválthat" – magyarázza[280] az FSZB a törvénytervezethez készült javaslatában. A támadás lehetséges forgatókönyveire a Stuxnetet hozzák fel példaként, illetve „néhány délkoreai vezető pénzintézet 2013. márciusi megbénítását".

Az FSZB részéről a törvénytervezetet és a kritikus infrastruktúra védelmét a hivatal igazgatóhelyettese, Dmitrij Salkov felügyelte. 2017 januárjában bejelentette, hogy az elmúlt egy év alatt az orosz informatikai erőforrásokat külföldről hetvenmilliószor támadták meg (Vlagyimir Putyin ugyanezt a számot említette, amikor a 2015-ös évről beszélt).[281] „Az orosz infrastruktúra folyamatosan ki van téve hekkertámadásoknak. 2016 novemberében összpon-

tosított támadást hajtottak végre az ország pénzügyi szektora ellen. A támadás célpontja a Sberbank, az Alfa Bank, a Bank Moszkvi és mások voltak. A támadásokat az FSZB informatikai biztonsági szakértői semlegesítették. A kritikus orosz erőforrások elleni támadások száma folyamatosan nő" – fejtette ki[282] Salkov, amikor az állami duma elé terjesztette a törvénytervezet.

A törvénytervezetet első olvasatban[283] 2017. január 27-én fogadták el, azonban a tárgyalás második szakaszát többször is elnapolták. Július 23-án az FSZB vezetője, Alekszandr Bortnyikov kérte[284] az ügyosztályt, hogy gyorsítsák fel a kritikus infrastruktúráról szóló törvénytervezet elfogadását, mire az két hét múlva, 2017. július 7-én átment második olvasatban, és vele együtt végül elfogadták[285] az államtitokról szóló törvény módosítását is. Ezeket kiegészítették a kritikus informatikai infrastruktúra biztonsági intézkedéseivel és azok kibertámadás elleni védelmével. Néhány nap múlva a törvényt Vlagyimir Putyin aláírta.

2019 februárjában az orosz hatóságok azt a döntést hozták, hogy elszigetelik az internet orosz szegmensét, és megszűrik az összes bejövő internetes információforgalmat. Most, ha feltétlenül szükséges, a hatóságok ki tudják kapcsolni az egész „külső internetet", azaz minden olyan weboldalt, amely nem orosz szervereken található. Az internetes szólásszabadság tiszteletben tartását felügyelő Roszkomszvobodi nevű szervezet igazgatója úgy véli,[286] ez a lépés csak egyik eleme annak a stratégiának, amelynek révén a hatalom megpróbálja bebiztosítani magát a tiltakozások ellen: ezek résztvevői ugyanis általában az interneten keresztül hangolják össze tevékenységüket.

* * *

A kritikus infrastruktúra védelmére szolgáló eszközöket számos kereskedelmi társaság dob piacra: ilyen a Positive Technologies, a Kaspersky Lab és a Group-IB283.[287] Az Informzascsita hosszú évek óta dolgozik együtt az államl-



mal, például a szocsi olimpia ideje alatt megbízást kapott a közlekedés biztonságának védelmére. A *Forbes* magazin szerint[288] az Informzascsita öt év alatt négyszázötven szerződést kötött állami megrendelőkkel mintegy ötmilliárd rubel összértékben.

Az Informzascsita alapítói a katonai kutatóintézetek vezérkarából érkeztek (a Kvantumból is). Az 1990-es évek végén kezdték kiépíteni saját védelmi rendszerüket a központi választási bizottságban és a központi bankban, a 2000-es években pedig kibocsátották a hálózatok és a rejtjelezett adatok védelmére szolgáló eszközt, a Kontinentet, amelyet számos állami szerv használ.[289] Ugyanakkor az Informzascsitán belül megjelent a pentesterek* osztálya: mielőtt a cég a programjait eladta volna a megrendelőknek, letesztelte a rendszere stabilitását.

Az Informzascsitával mások mellett Alisza Sevcsenko is együtt dolgozott:[290] az ő cégét, a COP Securityt az USA védelmi minisztériuma a 2016 decemberében szankció alá vonta az elnökválasztásba való beavatkozás miatt.

Instagramján Sevcsenko „kedves hekkerlánynak" nevezte magát.[291] Egy ismerőse úgy jellemezte, mint Oroszország egyik legtehetségesebb behatolástesztelőjét, aki szinte minden rendszert fel tud törni. Szerinte Sevcsenko nagyon sokat dolgozik, és minden szabadidejét a szakirodalom olvasásával tölti. Honlapja szerint „a leggyakrabban a sérülékenységek elemzésén és exploitokon dolgozik". 2014 tavaszán, az orosz hekkerek évi rendes fórumán, a Positive Hack Daysen könnyedén törte fel a városi gyakorlótér infrastruktúrájának igazgatási rendszerét, amelynek a védelmét „triviálisnak" nevezte.

Sevcsenko a Kaspersky Lab vírusanalitikusaként kezdte karrierjét,[292] ezt követően megalapította saját cégét, az Esage-t, amely szervezetek informatikai biztonságának elemzésére szakosodott. A cég a DialogNauka nevű in-

* Lásd *Fogalomtár.*

tegrátortól kapta megbízásait, amely a szövetségi rendőrséggel és a védelmi minisztériummal áll szerződésben. Az Esage-t később Számítógépes fegyverkezés és védelem névre keresztelték át, és a behatolások tesztelésével kezdett foglalkozni, phishing leveleket és kártékony honlapokat használva ehhez (tehát ugyanazokat a módszereket, amelyeket az amerikai politikusok és a nemzetközi sportért felelős hivatalnokok rendszereit megtámadó hekkerek is használtak).

Körülbelül tíz ember dolgozik Sevcsenkóval, mindannyiukat a hekkerfórumokon találta meg. Ahogyan arra a *Forbes* magazin rámutatott,[293] a feltörések érdekében közösen dolgozzák ki az eszköztárukat. Az Egyesült Államok hatóságai úgy vélik,[294] Sevcsenko cége a GRU számára bocsátja rendelkezésre kutatásait és fejlesztéseit. „Olyan, valami listáról szóló tonnányi megkeresésre ébredtem, amelyekről soha nem hallottam – írta Sevcsenko a Twitterére, egy nappal az USA védelmi minisztériumának közleménye után. – Úgy látszik, ma sem fogok lógni..." Egy ismerőse arról számolt be nekem, hogy Sevcsenko elhagyta Oroszországot, cége honlapja[295] jelenleg nem elérhető.

*34. fejezet*

## Az összvilági zsaroló

A Kaspersky Lab irodája a khimki víztározó partján fekszik, nem messze a „Vízistadion" metrómegállótól: a három hatalmas új épületet a cég 2013-ban szerezte meg háromnegyedtízmillió dollárért. Az épületek mögött két futballpálya terül el, kis utak vezetnek a parthoz, ahol a cég munkatársai séta közben is tarthatnak munkamegbeszéléseket. Nem messze [illegible] röplabdapályákat, így az ebédszünetekben sokan fogják a kávéjukat, és kimennek a lelátóra.

Amikor 2017. május 12-én az egész világon elterjedt a WannaCry *zsarolóvírus*, a Lab épületei gyorsan kiürültek: A fertőzött kliensekhez még azok a munkatársak is elindultak [ti. vírust irtani – a szerk.], akik egyébként az irodában ülnek. Az egyik munkatárs szavai szerint „speciális kisbőröndöket" hordanak magukkal, amelyekben benne van mindenféle pendrive, vezetékek, „tiszta" merevlemezek, energiaszelet és egy üveg kávé.

A Lab telefonjai folyamatosan csörögtek, de a munktársak nem voltak ehhez elegen. „Péntek volt, azt mondtam a telefonálóknak, jöjjenek inkább szombaton, ők meg azt válaszolták, hogy nekünk mindegy, az a lényeg, hogy hétfőre minden működjön" – emlékszik vissza Szergej Golovanov.

A következő néhány nap alatt a WannaCry körülbelül kétszázezer számítógépet támadott meg: Németországban a Deutsche Bahn vasúttársaságot, Franciaországban a Renault autógyárat, Japánban a Nissant, Spanyolországban a Telefónica nevű telekommunikációs társaságot, Nagy-Britanniában pedig az állami egészségügyi rendszert. Orosz-

országban a vírus a MegaFon telefonszolgáltató céget fertőzte meg, emiatt a munkatársak nem tudták használni a társaság belső rendszerét. Szintén Oroszországban a vírus néhány rendőrőrs számítógépeit is kódolta, aminek következtében az őrsön nem tudták kiadni a vezetői engedélyeket.

Saját rejtjelező vírusukkal együtt a WannaCry létrehozói a támadásoknál az EternalBlue exploitot használták, amelyet az amerikai NSA hozott létre. Ezek az exploitok tették lehetővé, hogy gyorsan és sikeresen terjedjen a vírus. Az EternalBlue 2016. április 14-én vált nyíltan hozzáférhetővé, miután a Shadow Brokers csoport hekkerei nyilvánossá tették. Meg voltak róla győződve,[296] hogy ugyanannak az amerikai titkosszolgálathoz tartozó alosztálynak a fejlesztéséhez férnek hozzá, amely a Stuxnetet is kifejlesztette. A Microsoft elnöke (a program éppen a Windows támadhatóságait használta ki) mindezt egy Tomahawk szárnyas rakéták ellopásának elvi lehetőségével hasonlította össze.[297]

Egy hónap múlva, 2017 júniusában, a WannaCry egy hasonló vírussal együtt végrehajtotta a történelem legpusztítóbb és legnagyobb anyagi kárt okozó kibertámadását.

A NotPetya nagyon egyszerűen működött. A vírus bekerült abba a számítógépbe, amely a Windowsszal dolgozik, letöltötte az internetről a programot, és rejtjelezte a merevlemezt, blokkolva ezzel a hozzáférést. Ezután a számítógép a felhasználónak a „képernyő kék halálát" mutatta, és váltságdíjat követelt: azért, hogy az adatok ne semmisüljenek meg, a bűnözők a háromszáz dollárnyi bitcoint kértek a visszaállításért. A vírus egy szempillantás alatt elterjedt: ha bekerült a helyi hálózat egyik számítógépébe, gyorsan megfertőzte az összes többit is.

A NotPetyának elnevezett vírus első áldozataivá ukrán vállalatok váltak, de hamar csapást mért az egész világra amerikai kórházaktól tasmániai csokoládégyárakig. Oroszországban a Rosznyeft és az Evraz szenvedte meg a



támadást. „Nálunk a teljes gazdaság nemzetközi, épp ezért a vírus az egyik irodától átfolyik a másikba, mindössze néhány perc alatt" – magyarázta a Kaspersky Lab. A *Wired* magazin adatai szerint a vírus okozta összes kár a tízmilliárd dollárt is elérte.

A NotPetya vírus kifejlesztéséhez a Mimikatz nevű programot használták fel, amelyet egy francia programozó, Benjamin Delpy írt. Elbeszélése szerint[298] 2013-ban Moszkvában egy információbiztonsági konferencián szerepelt egy program prezentációjával, és amikor visszament a hotelszobájába, egy fekete ruhás férfit talált bent, aki Delpy bekapcsolt notebookja mellett állt. Az ismeretlen megpróbált belépni a rendszerbe, de amikor észrevette a szoba lakóját, azt mormogta, eltévesztette a szobát, és hogy az ő kulcsa nyilván véletlenül nyitja Delpy ajtaját is, azzal elment.

Az Egyesült Államok és Nagy-Britannia titkosszolgálatai kijelentették,[299] hogy a NotPetya vírus mögött a GRU-hoz tartozó orosz katonák állnak. A támadások eredeti célja láthatóan Ukrajna pénzügyi rendszere volt.

Az Oroszországi Föderáció Biztonsági Tanácsának helyettes vezetője, Oleg Hramov közölte,[300] hogy az orosz kritikus infrastruktúra a GoszSZOPKA-nak köszönhetően egyáltalán nem szenvedett kárt a WannaCrytól és a NonPetyától. Egyébként a szakemberek biztosak abban, hogy ez nem az utolsó támadás volt.

„Ez csak egy bemutató volt, egy jövőbeni hatalmas méretű kiberháború demóverziója – írta jelentésében[301] a Group-IB a WannaCryról. – Világossá vált, mennyire sebezhető a jelenkori világ a titkosszolgálatok és a kiberhadseregek által kifejlesztett számítógépes fegyverzettel szemben, amikor ez az arzenál már nem az ő kezükben van. Sajnos az emberiség egész történelme azt mutatja, hogy a katonák állandóan egy új háború várakozásában élnek: a külső ellenség létezése lehetővé teszi a büdzsé felduzzasztását és azt, hogy a váll-lapokra új csillagok ke-

rüljenek. A vicc az, hogy bármely háború, beleértve azt is, amely a kibertérben zajlik, a technológia jelenlegi fejlettsége mellett az emberiség számára az utolsó lehet."

* * *

Ilja Szacskov azon kevés szakértők egyike, akik beleegyeztek abba, hogy saját néven beszélgessenek velem az orosz hekkerekről – és azok lehetséges állami kapcsolatairól. Szacskov alapította a Group-IB társaságot. 2016. október elején ő szervezte Moszkvában azt a konferenciát, amelyen ugyanúgy részt vettek az Interpol képviselői, mint az FSZB és a belügyminisztérium „K" ügyosztályának munkatársai. Ezt követően a hekkerek váltak a média egyik fő témájává. Szacskov állandó hőse lett a bulvárlapoknak, még fotósztorit is készítettek vele.

A GROUP-IB irodája több emeletet foglal el egy Moszkva központjától nem messze eső épületben. A felderítést végzők szobájában az internetaktivisták szimbóluma, Anonymous lóg a falakon, Szacskov dolgozószobájának falán pedig az FSZB-től és a belügyminisztériumból kapott elismerések a segítségnyújtásért. Szacskov harminc körüli; a Bauman műszaki egyetem kibervédelem szakán végzett, az irodába egy notesszal jár, amelyre a Szputnyik orosz propagandaoldal címkéje van ráragasztva, a következő felirattal: *Telling the Untold.**

Szacskov véleménye szerint a világban „kiberháború zajlik", és az orosz állam „hülye lenne nem létrehozni a saját kiberparancsnokságát és tudományos századait". Szacskov azt mondja, hogy a védelmi minisztérium láthatóan beletörődik és bele is fog ütközni a számára szükséges szakemberek felkutatásának problémájába: „a védelmiseket" az internetes gigavállalatok, a bankok és a kereskedelmi vállalatok is felbérlik kiberbűncselekmények felderítéséhez.

* Elmondani az elmondhatatlant. – *A szerző megjegyzése.*



„A hidegháború befejeztével a kémkedés története nem ért véget" – fejtegeti Szacskov. Ő azt reméli, az orosz állam nem működik együtt a hekkercsoportokkal. Véleménye szerint a hekkereket csak akkor lehet ellenőrizni, ha beülünk a szobájukba, rájuk szegezzük a Kalasnyikovot, illetve megfélemlítjük őket: vagy a börtön, vagy a feladatok teljesítése. Meggyőződése, hogy a kiberfegyverkezés nagyon hamar kikerülhet a kontroll alól: a csapásokat nem a honlapokra vagy a személyes levelezésekre fogják mérni, hanem a legkomolyabb objektumokra, például az ország kritikus infrastruktúrájára vagy annak pénzügyi rendszerére.

„Általában amikor a (hekker)csoportok észreveszik, hogy megfigyelik őket, teljesen megváltoztatják a struktúrájukat (ez a saját maguk megtámadása). A Fancy Bear egy sor rá visszaható feltörést hajtott végre, de egyébként nem bonyolult ezeket a támadásokat egymás között összehangolni: azonos algoritmus mentén működnek – fejtegeti Szacskov. – Ők (a Fancy Bear) vagy idióták, vagy nem félnek."

– Azaz meg vannak győződve róla, hogy büntetlenek maradnak?

– Igen.

*35. fejezet*

## Kémkednek utánunk

2016 májusában Roman Udot meg volt győződve arról, hogy lehallgatják a telefonját. Udot régóta annál a Golosz* nevű watchdogszervezetnél dolgozik, amely a választási szabályok megsértését követi figyelemmel (és borzasztóan idegesíti az orosz hatóságokat). „Ha érdekvédő vagy, akkor a telefonodat lehallgatják, ez olyan egyszerű, mint az, hogy kétszer kettő négy – mondja. – Hogy egy beszélgetésből megtudják, hová járok vacsorázni a barátaimmal? Ez az ára annak, amivel foglalkozunk. És ebbe muszáj beletörődni."

Az utóbbi időben a Golosz több találkozóján és rendezvényén, amelyeknek helyszínét és időpontját nem szokták nyilvánosságra hozni, megjelentek az állami NTV tévécsatorna munkatársai, mégpedig arról az osztályról, amely szenzációhajhász leleplező filmeket forgat az orosz ellenzékiekről (a Goloszról készült film 2016. június 3-án került adásba).

Ekkor Udot és a kollégái úgy határoztak, hogy tesznek egy kísérletet. A Golosszal e-mailen keresztül érintkezésbe léptek a kanadai nagykövetség képviselői. Kértek egy találkozót a soron következő parlamenti választásról és a szervezet munkájáról szóló beszélgetésre. Általában az ilyen találkozók a nagykövetségen vagy egy kávézóban zajlanak, de ez alkalommal a diplomaták azt javasolták, hogy a civil szervezet irodájában találkozzanak. A helyet

* Magyar jelentése: hang. – *A fordító megjegyzése.*



és az időt telefonon rögzítették, hogy ellenőrizni tudják, megjelennek-e a találkozón az NTV munkatársai.

Amikor a kanadaiak megérkeztek az irodába, az épület mellett szinte azonnal megjelent a tévétársaság autója. Az Udottal való beszélgetés során az NTV munkatársai azt mondták, nem hallgatják le a telefonját. Néhány nap múlva az Egyesült Államok korábbi oroszországi nagykövete, Michael McFaul felismerte őket: ugyanazok voltak, akik 2012-ben olyan rendezvényeken jelentek meg, amelyeknek a megtartásáról semmiféle előzetes értesítést nem küldtek ki. Az amerikai külügyminisztérium akkor azt feltételezte, hogy a tévétársaság megszerezte a hozzáférést a nagykövet naptárához, feltörték a postáját vagy a telefonját.

Az informatikai védelem területén működő egyik orosz cég szakértője azt magyarázta nekem, hogy a titkosszolgálatok Udot után valószínűleg az úgynevezett SZORM-on keresztül kémkednek (azaz a lehallgatásokhoz használt apparátus segítségével, amelyet az FSZB műveleti munkatársai a bíróság döntése alapján használnak), vagy a telefonjára telepített kémvírussal. Van azonban még egy variáció: a lehallgatás megvalósulhat a mobilhálózat támadhatóságán keresztül is, amiről csak az információbiztonsági és a a távközlési szolgáltató tudnak: „rések" vannak az SS7 protokollrendszerében, amit a telefontársaságok a szolgáltatásparancsok továbbításához használnak. E támadhatóság révén egy nem túl bonyolult feltörést követően lehet fogni és le lehet hallgatni a hívásokat, nyomon követhető az előfizető tartózkodási helye, el lehet olvasni, sőt le is lehet másolni az sms-eit.

Támadás gyakorlatilag bármelyik telefontulajdonost érheti: politikust, jogvédőt, újságírót, üzletembert, egy féltékeny férj feleségét, egy féltékeny feleség férjét, vagy bárki mást a világ hét és fél milliárd mobiltelefon-előfizetője közül. A hekkerek bármely kommunikációs rendszerű telefont képesek megtámadni: a régi nyomógombosakat is, az

okostelefonokat is, az iOS és az Android operációs rendszert használókat is.

Az SS7-en keresztül bekövetkező támadástól a világ mobilszolgáltatóinak körülbelül a 90 százaléka nem védett (biztonságban olyan szolgáltatók állnak, amelyek lecserélték a kiöregedett protokollokat, és azok, amelyek a kártékony tevékenységek leleplezése érdekében folyamatosan analizálják előfizetőiket). Az előfizetők sms-üzeneteinek a 89 százalékát el lehet fogni, az előfizetők 58 százalékát meg lehet figyelni, az előfizetők felének a beszélgetéseit le lehet hallgatni. Erről írt a Positive Technologies orosz cég az egyik jelentésében, amelyben a világ legnagyobb mobiloperációs rendszereit vonta vizsgálat alá.

***

Az SS7-protokollokat az 1970-es években kezdték kidolgozni. Ekkoriban a rádióamatőrök olyan önállóan működő készülékek konstruálásáért lelkesedtek, amelyek segítségével sikerült imitálniuk a telefonközpontok közötti jelek továbbítását (ez volt a „központok közötti jeladás"), és sikerült azokra a szükséges parancsokat elküldeniük. Az ilyen készülékek, amelyek „kék dobozok" néven váltak ismertté, lehetővé tettek hívásokat bárhova, miközben a hívásokért helyi tarifáért fizettek. „A kék dobozokat" például az *Apple* megalapítói, Steve Jobs és Stephen Wozniak a saját garázsukban rakták össze.

A telefontársaságok a csalók elleni harc érdekében szétválasztották az előfizetőket (hangátvitel) és a szolgáltatási forgalmat (technikai parancsnok). Így jelent meg az SS7, az információcsere és a hívásirányítás (milyen számot hívnak, kit, honnan stb.) érdekében létrehozott jelzőrendszer-protokoll.

Ezt a metróhoz hasonlíthatjuk: az SS7 olyan, mint ott a dolgozók szolgálati alagútja, az utasok által használt szerelvények nem itt járnak.

Az SS7 az 1980-es években kezdett működni, és a világ



összes távközlési szolgáltatóját egyesítette. Oroszországban, az Egyesült Államokban, Ázsiában és Európában a protokollokat különféleképpen hívják, de kompatibilisek egymással: egészében véve a rendszer a maga felépítésével az internetre emlékeztet. Oroszországban az SS7-et OKSZ-7-nek hívják (közös csatornajeladás №7), az USA-ban CCS7-nek, Németországban N7-nek, Nagy-Britanniában CCIS7-nek, de az általánosan elfogadott elnevezése az SS7.

A 2000-es évek elején kiegészítették az SS7-et a Sigtran nevű programmal, amely lehetővé teszi az információk és a parancsok továbbítását IP-hálózatokon keresztül: az SS7 hálózati komponensei elérhetővé váltak a nyilvános hálózatokon is, és néhányukhoz az interneten keresztül lehet csatlakozni. Az új és innovatív programvédelem a régi rendszerrel működött, amelyet egyáltalán nem védtek. Mi több, „rést" ütni ezen a rendszeren most még egyszerűbbnek tűnik.

Az SS7 sérülékenységéről szóló nyilvános diskurzus 2008-ban kezdődött. A Chaos Computer Club címmel rendezett hekkerkonferencián (amely az egyik legnagyobb a világon) az információbiztonság kutatója, a német Tobias Engel bemutatta[302] azokat az általa összegyűjtött módszereket, amelyekkel megfigyelhetők a mobilhálózatok előfizetői: ezek a megfigyelések az SS7-en keresztül történő behatoláson alapulnak. Úgy tűnik, a kormányzatnál és a titkosszolgálatoknál a támadhatóságról már korábban tudtak. Thomas Porter és Michael Gough telekommunikációs szakértők 2007-ben megjelent könyvükben arra mutattak rá, hogy az Egyesült Államok elnöki adminisztrációja komolyan aggódik egy SS7-en alapuló támadás nagyfokú fenyegetése miatt, egyéb amerikai dokumentumokban[303] pedig ilyen támadásokról már 1998 óta tettek említést. A támadhatóságról a mobilszolgáltatók fejlesztőinek is tudniuk kellett, de ezek általában tagadták a problémák létezését.

2013-ban a CIA és az NSA egykori munkatársa, Edward Snowden átadta a *The Guardian* és a *The Washington Post* újságíróinak azokat az archivált fájlokat, amelyek alátámasztották, hogy az Egyesült Államok és Nagy-Britannia titkosszolgálatai képesek megfigyelni bármely embert a bolygón (és élnek is ezzel a lehetőséggel). Ugyanebben az évben a *The Washington Post* arról számolt be,[304] hogy az NSA megfigyeléseinek alapját az SS7-en található „rések" adták. Egy év elteltével a lapok újságírói az SS7-en alapuló megfigyelés speciális programjairól tudósítottak[305] és arról, hogy az SS7 segítségével a hekkerek „meg tudják határozni[306] a felhasználó tartózkodási helyét a világ bármely pontján, le tudják hallgatni a beszélgetését, amikor az zajlik, vagy le tudják jegyezni a rejtjelezett hívásokat és a szöveges üzeneteket egy későbbi kódfejtés számára".

Az első években SS7-hozzáféréssel a kiválasztott kereskedelmi és állami telefontársaságok rendelkeztek. A 2010-es évek végén már az SS7-hez legálisan kapcsolódók számát meghatározni is lehetetlen: (virtuális) mobilszolgáltatók és szórakoztatóipari tartalomszolgáltatók egyaránt vannak közöttük. Az ilyen cégeknél százezernyi ember dolgozik, s közöttük lehetnek nem lojális, de kellő tudással rendelkező munkatársak.

* * *

2014-ben orosz kibervédelmi szakértők, Dmitrij Kurbatov és kollégája, Szergej Puzankov megvizsgálta, vajon találni-e olyan operációs rendszert, amely ismeretlen embereket kapcsolhat az SS7-hez. Miközben dél-amerikai és közép-ázsiai mobilszolgáltatók képviselőivel beszéltek, kiegészítő szolgáltatások kezdő tartalomszolgáltatóinak tették magukat, akiktől azt várják, hogy azért kapcsolódjanak rá az SS7-re, hogy „az előfizetőknek szétküldhessék a legjobb időjárás-előrejelzést". Több szolgáltató beleegyezett, hogy hivatalosan megadja nekik a hozzáférést, mások négyezer dollár ellenében ajánlották fel a rákapcsolást. Kurbatov szavai szerint, ha bármely telekommunikációs



társaságnál vannak ismerőseid, az SS7-hozzáférést nagyon könnyű megszerezni.

Az előfizetők elleni támadásokhoz nincs szükség bonyolult felszerelésre. „Nem kell hozzá zseninek vagy hírszerzőnek lenni – mondja Kurbatov. – A program egészét mi magunk írtuk meg, kiegészítve azzal, amit az internetről töltöttünk le. A belépési küszöb alacsony."

Elég egy megfelelő szoftver segítségével megtudni a SIM-kártyához tartozó IMSI-kódot, azét a speciális azonosítóét, amellyel minden mobil-előfizető rendelkezik (ez az ország és a szolgáltató kódját, valamint a SIM-kártya egyedi számát tartalmazza). Ezzel egyidejűleg a hekker megkapja az MSC/VLR paramétereit (azaz a hívások házi telefonközpontját és a tartózkodási helyet), amelyek révén az előfizető fenn van a hálózaton.

Mindehhez az szükséges, hogy „becsapjuk" az előfizető „házi" hálózatát és áttegyük azt a sajátunkba, a hamisba. A „házi" hálózat esetén ez úgy fog kinézni, mintha az előfizető (a „cél") elutazott volna, és a roamingot veszi igénybe (vagyis egy másik országban használja az otthoni SIM-kártyáját), csakhogy maga az előfizető erről soha nem értesül. A hamis hálózat parancsot ad a szolgáltatónak, hogy mostantól ő szolgálja ki az előfizetőt (azaz a szolgáltató kap egy olyan jelet, hogy az ő előfizetője egy másik mobilszolgáltató kiszolgálási zónájában van). Ezután a speciális program segítségével a hekker megkaparintja az sms-eket, le tudja hallgatni a hívásokat, és követheti a „cél" tartózkodási helyét.

Kurbatov azt mondja, az ilyen hozzáférést csak a legritkábban használják megfigyelésekhez, sokkal gyakrabban ahhoz, hogy pénzt lopjanak a mobilpénztárcákból és az sms-banking rendszereken keresztül az ügyfelektől: ez általában nem nagy pénz, de bűnözői csoportok ezt még megforgatják.[307]

Miután megszerezte az SS7-hez a hozzáférést, a hekker eltulajdonítja[308] az azonosítókódokat a Telegramtól, a

WhatsApptól, valamint a kétfaktoros jogosultsági jelszavakat a Gmailhez, a Facebookhoz és a VKontaktéhoz. Miután kezdeményezte a Telegramhoz való csatlakozást, a bűnöző sms-ben megkapja a belépéshez szükséges kódot az „eltérített" telefonra, aminek révén teljes értékű hozzáférést kap a messengerhez. Így tud az előfizető nevében üzenetet írni, el tudja olvasni a levelezését, amelyet a Telegram automatikusan letölt az új telefonra. Elzárva csak a titkosított chatek maradnak. A WhatsAppon a régi levelezést nem sikerült elolvasni: ezt nem tárolják a szerveren, és 2016 áprilisától a WhatsApp minden felhasználónál bekapcsolta a teljes kódolást.

„Minden, ami sms-sel van összefüggésben, feltörhető attól a pillanattól, amikor az SS7 működésbe lépett – mondja Karsten Nohl, német hekker.[309] – A mobilhálózat nyilvánvalóan a leggyengébb láncszem a digitális védelmünkben."

Az áldozatok ritkán értesülnek arról, hogy feltörték őket. A kibertámadások elleni programok kidolgozásával foglalkozó amerikai FireEye társaság kutatásai szerint[310] egy hekker a feltört hálózaton vagy accountban a leleplezésig átlagosan kétszázöt napig tartózkodik.

2016. április 29-én éjjel Oleg Kozlovszkij ellenzéki politikus és Georgij Alburov, a Korrupcióellenes Küzdelem Alapítvány munkatársa, mindketten MTSZ*-ügyfelek, közölték, hogy Telegram-fiókjukat feltörték. Ismeretlenek sms-eket fogtak be az ő fiókjaik jelszavaival. Ez elegendő volt ahhoz, hogy belépjenek a rendszerbe, viszont az ellenzékiek ne léphessenek be saját jelszavaikkal a kettős jogosultsággal védett fiókjaikba. Kozlovszkij és Alburov nem kapott sms-értesítést a (jogosulatlan) belépésről. Kozlovszkij azt mondta, az MTSZ fiókja feltörésének pillanatában kikapcsolta az sms-küldés-szolgáltatást. A segélyszolgálatnál állítólag közölték:[311] „A rövid szöveges üzenetek szolgáltatását önnél kikapcsolta a műszaki vé-

* MTSZ: Orosz Telekommunikációs Társaság rövidítése.



delmi osztályunk." Később az aktivisták kiposztolták a 2016. áprilisi szolgáltatásokról szóló nyugtákat: ezekben mind Kozlovszkijnál, mind Alburovnál történt utalás arra, hogy kikapcsolták az sms-szolgáltatást. Az MTSZ ezt cáfolta, a cég képviselője, Dmitrij Szolodovnyikov pedig azt mondta:[312] „Semmiféle célirányos tevékenység a szolgáltatás kikapcsolására nem történt. Nem zárom ki egy vírustámadás vagy egy internetes felületen keresztüli fiókhozzáférés valószínűségét." Lehetséges, hogy ugyanilyen módon hallgatták le az Egyesült Államok külügyi államtitkár-helyettese, Victoria Nuland beszélgetését is az USA kijevi nagykövetével, Geoffrey Pyatt-tel; a telefonbeszélgetésükről szóló feljegyzést ismeretlenek közzétették. Az első utalást a hanganyag feljegyzésére Dmitrij Rogozin orosz miniszterelnök-helyettes tanácsadója tette.

Ha az ellenzékieket az SS7-en keresztül támadták meg, akkor a hekkerek képesek voltak ezt úgy megtenni, hogy a feltört előfizetőkhöz ne érkezzen sms-értesítés.

Az SS7-en keresztüli támadással a hívások és az üzenetek elfogása mellett a hekker ki tudja vezetni a telefont a rendszerből: a készülék azt mutatja, hogy fogja a jelet, mégsem lehet az illetőt telefonon elérni. Az ilyesfajta támadások üzletembereket károsíthatnak meg egy tárgyalási folyamat ideje alatt, és újságírókat, akik épp kapcsolatban állnak a forrásaikkal. Ezeket a módszereket ugyancsak alkalmazhatják fegyveres konfliktusok idején.

Az orosz titkosszolgálatok régóta foglalkoznak kémvírusok létrehozásával, amelyeket telefonokra telepítenek. Ehhez általában fizikai kontaktusra van szükség a készülékkel. Vannak egyébként más módszereik is a megfigyelésre, amelyek nem igényelnek bonyolult mesterkedéseket: például használni tudják a SZORM-ot, azaz a műveleti és nyomozati intézkedések biztosítását szolgáló műszaki eszközrendszert, amely sok minden más mellett azt is lehetővé teszi, hogy kövessék a telefonbeszélgetéseket vagy az internetes információáramlást. Az orosz törvényhozás

szerint a titkosszolgálatoknak csak bírói engedély alapján van joguk működtetni ezt a rendszert, azonban 2012-ben Oroszország legfelsőbb bírósága törvényesnek ítélte[313] a titkosszolgálatoknak azt a jogát, hogy lehallgathatják az ellenzékieket, pusztán azon az alapon, hogy azok tiltakozó tevékenységet folytatnak. Az orosz *Forbes* kutatásai arra mutattak rá,[314] hogy az FSZB munkatársai a lehallgatásra vonatkozó határozatot senkinek sem kötelesek megmutatni: a telefonszolgáltatóknak nincs joguk tudni, kinek a beszélgetéseit vagy e-mailjét fogják el a titkosszolgálatok. A SZORM igazgatási pontjait védett kábelen keresztül kapcsolták össze a mobilszolgáltatók és az internetszolgáltatók szervereivel, a lehallgatáshoz így az FSZB munkatársainak elég betáplálniuk a parancsokat a SZORM igazgatási pultjánál, amely a hivatal helyi igazgatási épületében helyezkedik el.

*36. fejezet*

## Az anonimek az állam ellen

2018. március 4-én ismeretlenek feltörték a V. P. Makejev akadémikus nevét viselő Állami Rakétacentrum honlapját. Ez a centrum fejlesztette ki azokat az „előre nem jelezhető" rakétákat, amelyekkel Vlagyimir Putyin az orosz parlamenthez intézett felszólalásakor dicsekedett. A megszokott címlap helyett a honlapon egy sötét bőrű, BDSM-öltözetbe bújt férfi képe jelent meg, mellette a felirat: *„putyin, kész a saját rakétám"*.

Egyébként a weboldal gyorsan visszanyerte eredeti formáját, később pedig már nem törték fel. Az utóbbi években az „ellenzéki" hekkertámadások száma jócskán megcsappant – a támadások virágzása a 2010-es évek első felére tehető, ami után az orosz állam valóságos kiber-polgárháborút hirdetett a támadókkal szemben.

2012 februárjában ismeretlen hekkerek feltörték a Roszmologyezs* vezetője, Vaszilij Jakemenko postafiókját. Jakemenko a Kreml-barát fiatalok mozgalmainak ideológusa és alapítója, amelyeket a „narancsos forradalom" és az ellenzék elleni harc „nulladik napján" hoztak létre. Jakemenko levelezését kiposztolták a #OpYoungBustards alatt és néhány blogon: a KremlinGate-n, az UltraZashkvaron, a Rumol-Leaksen. Minden másnál érdekesebb volt Jakemenko levelezése a Roszmologyezs sajtótitkárával, Krisztina Potupcsikkal, aki régi, oszlopos tagja a Mieink mozgalomnak.

A levelezésből kiderült, hogy Jakemenko egy DDoS-

* Szövetségi Ifjúsági Ügynökség.

támadás megszervezéséről és az ellenzékiek postafiókjainak feltöréseiről tárgyalt a bajtársaival. Levelezésének jelentős része fizetett tartalmak elhelyezéséről szólt népszerű orosz blogokon – ezekre százezreket költöttek. A legtöbbért állítólag Ilja Varlamovnál lehetett posztolni: körülbelül négyszázezer rubelbe került az a két anyag, amelyek egyike Putyin látogatásáról szólt a 2011-es Nemzetközi Repülési és Űrrepülési Szalonon, a másik pedig az Egységes Oroszország Párt kongresszusáról számolt be, amelyen bejelentették, hogy Putyin indul a harmadik elnöki ciklusért. Beszélgetésünk során Varlamov tagadta, hogy pénzt kapott volna a posztokért. Továbbá a „Köszönöm, Jeva" nevű projekt is kapott pénzt az államtól. A projektben vloggerek készítettek videókat. Közülük az egyik az a Danyila Poperecsnyij, aki egy propaganda-mesefilmsorozatot forgatott Vlagyimir Putyint támogatandó, és azt állította, nem tudta, milyen pénzből fizettek neki.

A levelezésből egyebek mellett sok minden kiderült a Jakemenkónak dolgozó fizetett kommentelőkről is – az ő tevékenységük az, amit róluk fognak „trollgyárnak" nevezni. Jakemenko és Potupcsik elhatározta,[315] hogy egy csoportba gyűjtik azokat az embereket, akiknek „fel van vágva a nyelvük, jól írnak és nem debilek", s kötelességszerűen „mocskolják az ellenzéket, és dicsőítik Putyint". „Ki kell alakítani azt a képet, hogy a többség mellettünk van" – fejtegették a levelezésben. Ezeknek a munkatársaknak a fizetése havi húsztól harmincezer rubelig terjedt, a pontos összeg a sikeres kommentelések és viták számától függött, egyeseket iPadekkel is megajándékoztak. Az ilyen kommentelőkre szánt kiadások, ahogyan azt az egyik jelentésben kimutatták, körülbelül hatszázezer rubelt tettek ki havonta.

Egy másik levélben Krisztina Potupcsik (a leveleket ugyanarról a címről küldték, amit a Zsivoj Zsurnalon tevékenykedő aktivisták személyes postájaként megadtak) állítólag a Kommerszant elleni DDoS-támadás megszervezését javasolta, hogy „megbénítsák öt órára a weboldalt, elviselhetetlen feltételeket teremtsenek, pszichológiailag és fizikailag is megsemmisítsék". A jelentésben, amelyet Jakemenko számára állított össze, Potupcsik rámutatott, hogy „azok a komoly erőforrások, amelyeket nem lehet teljesen likvidálni, ismétlődő, aktív DDoS-támadásoknak vannak kitéve".

Az egyik költségvetésben külön szerepelt egy bizonyos Arszen Mulmatmurzijev neve – az ő feladata úgy írható le, mint „azé az IT-specialistáé, azé a hekkeré, aki kivezeti a rendszerből az ellenfelek erőforrásait, feltöri a honlapokat és fiókokat". Havonta negyvenezer rubelt fizettek neki. Egy másik aktivista a Roszmologyezs vezetőjéhez írott levelében ajánlotta fel szolgálatait, azon „vezető bloggerek elleni [illegible] kidolgozását, akik állandóan negatív megjegyzéseket írnak, DDoS-támadást végeznek, és még „a legintimebb védett tartalmaikat is kivezetik a rendszerből". E szolgáltatásokért tizennyolcmillió rubelt kért évente.

Krisztina Potupcsik jelenleg egy könyves blogot jegyez, és polgári aktivistaként határozza meg magát. Vaszilij Jakemenko először az Egyél pirogot nevű kávézót nyitotta meg, azután könyvklubbal kezdett foglalkozni,[316] és vett egy házat Bajorországban.[317] A Roszmologyezs ügyleteinek más résztvevői államközeli tisztségeket töltenek be különböző orosz régiókban. A politikai ellenfelekkel folytatott harcok módszereit, amelyeket Oroszországban fejlesztettek ki, néhány évvel később az amerikai választásokon és az európai országokban alkalmazzák.

* * *

2014 áprilisában a Kreml-barát botokkal foglalkozó egyik szervezet vezetője a Mieink mozgalmárok egyik kedvenc helyét jelölte meg[318] találkozásunk helyszíneként. A bár a Szuharjovszkaja metrómegállóhoz esik közel.

Az illető 2011 decembere, a tömeges ellenzéki tiltakozások óta vesz részt az információs háborúban. Kezdetben

annyiból állt a munkája, hogy a „murzilka"* csoportot vezette: a csoport olyan újságírókból és bloggerekből tevődik össze, akik bizonyos összegért a Kreml számára előnyös híreket öntik végső formába, de közben nem írják ki a homlokukra, hogy a hatalomnak dolgoznak. Elmondása szerint mindennap szétküldi a murzilkának az elnöki adminisztrációtól kapott instrukciókat, vagyis olyan dokumentumokat, amelyekben leírják, hogyan és milyen hangsúlyokkal tálalják az eseményeket.

Az illető bizonyos delikvensekre az értelmiség körében népszerű kávézókban lelt. „Megérkezel, szétnézel: van, akinek pénzre lehet szüksége, van, aki talán nem teljesen szenvedélyes ellenzéki – mesélte. – Van olyan, akit beszervezés előtt kipróbáltak: tizenötezerért vajon leteszi-e a voksát egy bizonyos meglopott bibirjevói hivatalvezető mellett? Egy ilyen ember például így gondolkodik: hálás munka, és még pénzt is fogok kapni érte, a barátnőmet pedig a Zsan-Zsakba** fogom vinni. Te pedig folyamatosan mondod neki: „Állj ki Navalnij mellett." Az illető visszautasítja. Erre te: „Ha-ha, azt akarod, hogy mindenki tudomást szerezzen róla, hogy előre pénzt vettél fel ezért?"

Riportalanyom azt mesélte, hogy miután feltörték Krisztina Potupcsik postáját, mindenki rendkívül óvatos lett: titkos fiókokba regisztráltak, sőt, szuperkémeknek érezvén magukat, végig ellenőrizték, nem figyelik-e őket az üzleti partnereikkel folytatott tárgyalásaik alatt.

* A szó oroszul sok mindent jelent: kis termetű emberek gúnyneve, a törpe egyfajta elnevezése; a gyerekek kedvenc háziállatainak (kutyák, macskák) orosz összefoglaló neve; egy orosz irodalmi-művészeti folyóirat címe hat- és tizenkét év közötti gyerekek számára. Ezzel a kifejezéssel ellenzéki politikust vagy független újságírót is szoktak illetni, valamint: olyan embereket jelöl, akik rejtegetik a személyiségüket, és másnak adják ki magukat a világhálón. Az itteni csoportot is ezért hívják „murzilkáknak". – *A ford.*

** A Zsan-Zsak francia kávézó- és étteremlánc Moszkvában és Szentpétervárott, Jean-Jacques Rousseau nevéből. – *A ford.*



Az illető a megbízásért járó összeget készpénzben kapta, és efelett a saját belátása szerint rendelkezhetett: kivehetett egy irodát, felbérelhetett embereket. A szervezetén kívül hasonló dolgokkal Moszkvában 2014-ben még hét szervezet foglalkozott. Közös gyűléseiken több más mellett arról is tárgyaltak, mely ellenzéki honlapok ellen intézzenek DDoS-támadást, és kit fogadjanak fel az állambarát videók és tweetek megtekintései és like-jai számának manipulálására. Ennek érdekében például phishinget használtak, és olyan típusú leveleket írtak, mint például az „Ismerd meg a pszichológiai életkorodat" és hasonlók, amelyek révén könnyen hozzájutottak a fiókokhoz és használhatták azokat a választweetekhez.

A beszélgetés végén az interjúalanyom azt mondta mosolyogva, hogy Putyin legutóbbi sikereit figyelembe véve (a Szocsiban rendezett téli olimpiára és a Krím visszacsatolására gondolt) hamarosan munka nélkül maradhat. „Az információs háborúk mindegyikét lejátszottuk" – jelentette ki mély meggyőződéssel. Tévedett. Ha Oroszországban a botok és a hekkerek segítségére többet szinte nem is volt szükség, világviszonylatban hihetetlen sebességgel nőtt a támadásaik gyakorisága a soron következő években.

* * *

2012 februárjában azok a hekkerek, akik feltörték Vaszilij Jakemenko és más hivatalnokok levelezését, rábólintottak,[319] hogy érintkezésbe lépjenek velem egy kódolt chaten keresztül. Önmagukat az Anonymous orosz alosztályának nevezték. A kiberaktivisták nemzetközi mozgalma 2008 óta intéz támadásokat cégek, filmgyárak és szinkronstúdiók ellen, a szabadság jelszava alatt terjesztve az információkat. Azok az emberek, akik az Anonymousba tömörültek, aktívan részt vettek az úgynevezett arab tavasz eseményeiben, abban a forradalmi hullámban, amely a 2010-es évek elején végigsöpört a Közel-Kelet országain. Oroszországban pedig a tevékenységük nem szorítkozott

az állami szolgálatban állók és a Kreml-barát aktivisták közötti levelezésre. A hekkerek feltörték[320] az Egységes Oroszország Párt kaluzsszkajai kirendeltségének weboldalát is, és feltelepítettek rá egy videót, amelyben azzal fenyegették a hivatalnokokat, hogy folyamatosan megfigyelés alatt fogják őket tartani, illetve azzal kérkedtek, hogy őket magukat képtelenség megtalálni: lehet, hogy a hekker „az ön könyvelője, a postása, a titkára, az ügyvédje, sőt még az is lehet, hogy a fia".

„Az egyetlen cél, amit mindannyian osztunk, az internetes szólásszabadság megvédése – írta nekem az egyik hekker. – Nem köszönthet be az a nap, amikor egy »anonim« megengedi valakinek, hogy az lecserélje a gondolatait." A hekker elismerte, hogy többek között a Kreml hivatali honlapját is ők törték fel, bosszúból Alekszej Navalnij e-mailjének feltöréséért, amit egy Hell nevű hekker követett el.

2012 márciusában az „anonimek" DDoS-támadást szerveztek az NTV tévécsatorna honlapja ellen, ahol épp *Az ellenállás anatómiája* című propagandafilm ment (ebben arról adtak hírt, hogy az ellenzéki találkozók résztvevői pénzt kaptak az akcióikért). Az NTV weboldala tizenkét órán keresztül nem működött.

2012. május 6-án, a Bolotnaja téren tartott ellenzéki demonstráció idején, amely a rendőrséggel való összeütközéssel és a tiltakozók elleni bűnvádi eljárással végződött, az „anonimek" arra szólították fel szimpatizánsaikat, hogy támadják meg az elnök és a kormányzat honlapjait. Az újoncok számára részletes instrukciókat posztoltak ki, hogyan tegyék ezt, illetve hivatkozásokat az ehhez szükséges programokra. „Ezt a tiltakozást úgy támogatjuk, hogy kikapcsoljuk a hazug állami weboldalakat – elsősorban az orosz kormány weboldalát... Néhány egyszerű tett közelebb viszi ezt a korrupt rendszert a törvényszerű pusztulásához. A rendszer saját magát fogja felszámolni" – tették közzé kiáltványukban. Céljukat elérték: az állami honlapokat – beleértve az elnökét is – rövid ideig nem lehetett megnyitni.



Amíg bizonyos titkosszolgálatok a Bolotnaja-ügyet indították meg a találkozók résztvevői ellen, addig mások azok után kezdtek kutakodni, akik az interneten tiltakoztak. Alig egy hónap múlva az FSZB munkatársai Krasznojarszkban letartóztatták a rádióelektronikai főiskola húszéves hallgatóját, Pavel Szpasszkijt, és egy volt tisztviselőt, Vaszilij Nyikityint, Tomszkban pedig őrizetbe vették Szergej Tjuljupovot, egy helyi kisvállalat vezetőjét. Mindannyian kezdők voltak, egyáltalán nem értettek a hekkerkedéshez. Az Anonymous instrukcióit követve töltötték le a szükséges programokat, és beállították azokat egy DDoS-támadás számára. Mindannyiukat börtönbüntetésre ítélték,[321] Szpasszkijra két évet szabtak ki feltételesen, valamint huszonötezer rubeles pénzbírságot róttak ki rá. Nyikityin egy évet, Tjuljupov másfelet ült le.

Mindazonáltal az „anonimeket" ez nem állította meg. 2013 júniusában megkezdték a támadásukat a Roszkomnadzor (a telekommunikáció, az információs technológiák és a tömegkommunikáció szövetségi állami felügyelete) weboldala ellen: ez a hivatal felel az internet ellenőrzéséért is. Ezzel párhuzamosan az aktivisták a YouTube-on publikálták[322] az orosz emberekhez szóló kiáltványukat. Ahogyan külföldi kollégáik, az orosz hekkerek is elváltoztatott hangon tették ki felhívásukat a videómegosztóra, és minden egyes videójukon Guy Fawkes álarca, a megtorló kormányzattal szembeni harc szimbóluma tűnt fel.

*Hosszú évek óta* megaláztatásnak és nyílt gúnyolódásnak vagytok kitéve *az országotokban, odaadtok mindent, és cserébe semmit sem kaptok. A korlátlan jogi és törvényhozói hatalom, a korrupció, a hazug propaganda szakadatlan áradata, amely a televízióból ömlik rátok, oda vezetett, hogy sok ember úgy fogja fel, ez a normális, és nem is tudja másként elképzelni az életét, az ellenállókat pedig üldöztetésnek vetik alá.*

*Létezik azonban egy hely, ahol Oroszország* állampolgárai agyát eddig még nem tudták átmosni. *Ez az internet. Itt az ember mindig talál vele egyformán gondolkodókat, első kéz-*

*ből értesül olyan információról, amelyet nem vontak cenzúra alá, és saját maga vonhatja le a következtetéseit. De a gyerekek védelme és az online kalózkodás elleni harc leple alatt az állam valódi célja az, hogy cenzúra alá vesse az internethálózatot, és még több pénzt fordíthasson a net feletti ellenőrzést célzó kampányra. Akkor majd a valós hírek helyett ugyanazt a hazugságot fogjátok látni az interneten is, mint amit az „Egyes csatornán", miközben a kis fizetésetekből ti finanszírozzátok ennek a gyártását, amit úgy kínálnak fel nektek, mint „művészetet". Az, aki a szabad internetre akar kerülni, kénytelen lesz „megsérteni" a törvényt, és biztosan a börtönben köt ki.*

*Hogyha megengeditek, hogy elkobozzák tőletek az internetet, soha többé nem kapjátok vissza. Tiltakozzatok minden olyan törvény ellen, amely a hálózat adta szabadságotokra tör, ne engedjétek meg, hogy korlátozzák a szabad információcserét, és ne higgyetek az internet veszélyességéről szóló hazug kinyilatkoztatásoknak! Muszáj megérteni, hogy a világháló kontrollálására irányuló kísérletek az internetközösségre is hatással vannak: nem nyugszunk bele, hogy elvegyék tőlünk az internetet! Minden egyes elzárt weboldalért kettőt törünk fel, minden egyes hazugságra a leleplező igazsággal válaszolunk, minden egyes rendszabályra találunk ellenrendszabályt. Mi az Anonimek vagyunk, és rengetegen vagyunk. Nem bocsátunk meg, és nem felejtünk.*

Az „anonimek" figyelmeztetései helytállóknak bizonyultak, de az internetet mégsem sikerült megvédeniük: az utóbbi években az orosz hatóságok következetesen korlátozzák annak szabadságát.

* * *

Az a hivatal, amely az internet ellenőrzéséért felel – a Roszkomnadzor –, a Kitaj-Gorod nevű moszkvai városrész egyik hétemeletes, szürke kőlapokkal díszített épületében kapott helyet,[323] és kékes árnyalatú lucfenyők veszik körül. Ugyanitt székel a kulturális minisztérium. A Roszkomnadzortól az elnöki adminisztráció csupán ötpercnyi kényelmes sétára van.



2012 őszéig a hivatal tevékenységéről csak a szakmabeliek tudtak. A Roszkomnadzor 2008-ban alakult, ekkor vált le – alosztályként – a tömegkommunikáció felügyeletét ellátó és a kulturális örökség védelmét végző szövetségi szolgálatról. Ennek a hatáskörébe tartozott a tömegmédia felügyelete (beleértve a törvénysértésekre vonatkozó előzetes figyelmeztetések kiadását: azt a kiadványt, amely kettőnél több előzetes figyelmeztetést kapott, be lehetett tiltani), illetve ide tartozott a hírközlés felügyelete: a rádiófrekvenciákra vonatkozó licencek kiállítása, valamint engedélyek kiadása a tengeri rádióállomásokra és hírközlési vonalak építésére.

Igazából azt követően vált híressé a Roszkomnadzor, hogy 2012-ben elfogadták *A gyermekek védelméről* szóló törvény módosítását, amelyet „az egészségükre és a fejlődésükre káros" információk terjesztése ellen hoztak, s amelyet akkor még „feketelistás törvénynek" hívtak. Fő újításává *a domainnevek* és az oldalak betűrendes mutatóinak *egységes jegyzéke*, azaz a „tiltott információkat" tartalmazó honlapok listája vált, amelyet a felügyeleti szervek szakemberei állítottak össze. A jegyzéket a távközlési szolgáltatók részére hozták létre, amelyek kötelesek blokkolni a hozzáférést ügyfeleik számára a listán szereplő honlapokhoz. A törvénymódosítás egyik kezdeményezője az állami dumában az a Jelena Mizulina képviselő volt, aki a melegpropaganda tilalmáról szóló törvénnyel vált ismertté.

Az internettel kapcsolatos megtorló intézkedések ezzel nem értek véget. 2014. április 22-én az elnöki adminisztráció egyik munkatársának, Timur Prokopenkónak a postájába beesett egy üzenet a Kremlhez közel álló politológustól, Dmitrij Badovszkijtól (ezt onnan tudjuk, hogy Prokopenko postáját feltörték, és az interneten nyilvánosságra hozták). A levélhez csatoltak egy fájlt „internet_rö-

vid javaslat" címmel. A szövegben a következőről volt szó: „Az internet feletti kontroll mindmáig hivatalosan az Egyesült Államokhoz tartozik", kezükben van „az NSA totális megfigyelőrendszere". A politológus azt javasolta, „dolgozzanak ki és fogadjanak el [...] egy törvényt, amely arra kötelezi a külföldi internetes társaságokat, hogy az orosz felhasználók adatainak teljes feldolgozását kizárólag Oroszország területén szervezzék meg".

Két hónappal később be is terjesztették a törvényt az állami duma elé,[324] és gyorsan el is fogadták. Most minden olyan szolgáltatást, amely Oroszország állampolgárainak személyes adatait dolgozza fel, kötelesek orosz területen található szervereken futtatni.

2017 februárjában fogadták el a „Jarovaja-csomagot", amely többek között arra vonatkozó kötelezettséget írt elő,[325] hogy fél évig meg kell őrizni az összes feljegyzést a telefonhívásokról és más, a felhasználók közötti üzenetekről. Az internetszolgáltatók és az üzenetküldő szolgáltatások három éven keresztül kötelesek megőrizni a metaadatokat, azaz nem magát a beszélgetések és levelezések tartalmát, hanem az arról szóló információkat, hogy valamely beszélgetés vagy valamely üzenetváltás milyen dátummal és pontosan hány órakor történt. Ezek a szabályok érvényesek az „internethálózaton található információk terjesztésének szervezőire" is (hozzájuk tartoznak azok az internetes erőforrások is, amelyek egy fentihez hasonló jegyzékre vannak felvezetve). A metaadatok megőrzésének határideje az ő esetükben nem három, hanem egy év.

2017-re a Roszkomnadzor minden nap átlagosan kétszáznegyvennégy oldalt blokkolt[326] az interneten, a bíróság nyolcnaponta ítélt letöltendő börtönbüntetésre olyan embereket, akiket az Oroszországi Föderáció büntető törvénykönyvének 282-es cikkelye alapján szélsőséges nézetek kedvelésével vádoltak: emiatt évente több mint ötszáz ember került börtönbe (2018 végén megszűntek ezek a perek, miután a szóban forgó magatartást dekriminalizálták).



Az utóbbi öt év alatt a Roszkomnadzor több mint tízmillió weboldalt blokkolt.

Az „anonimek" aktivitása ez idő alatt majdnem a nullára csökkent. Utolsó támadásaikat 2014 tavaszán hajtották végre. 2014 márciusában az Anonymous, válaszul a lenta.ru főszerkesztőjének elbocsátására, megtámadta a Kreml weboldalát, amely egy ideig elérhetetlennek bizonyult. A Twitteren az anonimek ezt írták:[327] „A Kreml weboldala szar." Hamarosan támadást intéztek a külügyminisztérium, az Egyes csatorna, és a *Rosszijszkaja Gazeta* weboldalai ellen is. Amikor a weboldalak elérhetetlenekké váltak, örömüknek adtak hangot, és ezt írták a Twitterre: *„Tango down!"*

2015-ben néhány Twitter-aktivista fiókjait törték fel, 2016-ban egyik YouTube-csatornájuk pedig videókat kezdett el közzétenni az állambarát orosz Fancy Bear hekkercsoport nevében. Ezekben[328] a WADA* feltöréséről beszéltek, az amerikai sportolókat hazugsággal vádolták, és a nemzetközi sport megtisztítását követelték.

* Nemzetközi Dopping-ellenes Ügynökség. – *A szerk.*

*37. fejezet*

## A bangkoki összekötő

2014. augusztus 14-én tíz óra körül egy teljesen hétköznapi férfi betért a moszkvai Tisinszkaja tér szomszédságában az egyik kávézóba. Rendelt egy kávét, helyet foglalt a helyiség egyik távoli sarkában, kinyitotta a notebookját, és elindított néhány programot: egy szövegszerkesztőt, egy titkosított chatet és egy böngészőt. Aztán rácsatlakozott az ingyenes wifire, és a VPN-en fellépett a saját szerveréről – úgy, hogy a tevékenységét ne lehessen figyelemmel kísérni. Megnyitotta a böngészőn a Twittert, felvezette rá a felhasználói nevét és a jelszavát, amelyeket külön fájlban őrzött, és megírta az első tweetjét: *„Nyugdíjba vonulok. Szégyellem magam a kormány tevékenysége miatt. Bocsássatok meg."*

A bejegyzés Oroszország miniszterelnöke, Dmitrij Medvegyev hivatalos Twitter-fiókján jelent meg. Két és fél millió felhasználó látta.

Kávézása alatt a férfi megírt még néhány tweetet: *„Szabadúszó fotográfussá válok. Régóta álmodtam erről", „A kezdeményezéseink ellenére néhány hálózati huligán sza...k az útlevélhálózat-hozzáférésre ((»: „Régóta szeretném megmondani. Vova! Nincs igazad!", „Nekem tetszik, ha olvasom a @navalnyt."* Ezt követően visszatweetelt Alekszej Navalnij választási kampánystábja egykori vezetőjének, Leonyid Volkovnak, és az ellenzéki újságírónak, Roman Dobrohotovnak. Végül ezt írta: *„Azt gondoljátok, hogy Jaltában ma fognak mondani valami fontosat? Kétlem. Íme, itt ülök, és még én is azt gondolom, hogy semmit."*

A férfi nem úgy nézett ki, mintha valami rendkívüli dolgot csinálna. Eredetileg nem is gondolta, hogy ebbe a



kávézóba fog jönni, és írni fog a miniszterelnök fiókjára – egyszerűen nem volt más, akinek írhatott volna. Aznap ő volt az egyetlen az Anonimnij International csoportból (amelyet széles körben Saltaj-Boltajként ismernek), aki nem épp a főfoglalkozását űzte. A Saltaj hekkerei már régóta megszerezték a miniszterelnök Twitteréhez a kulcsot, amikor az iCloudból letöltötték Medvegyev három okostelefonjának elektronikus másolatát: a miniszterelnök a közösségi hálóhoz tartozó jelszavát az iPhone-feljegyzéseiben őrizte. A Twitter feltörését a csoport Vlagyimir Putyin jaltai beszédéhez időzítette. Az immár Oroszországhoz csatolt Krímben az elnök a kormányzat és a parlament előtt tartott beszédet.

„Medvegyevet két éve figyeltük, de semmi különös nem adódott, ezért úgy döntöttünk, hogy egyszerűen megtrollkodjuk" – magyarázta nekem a feltörés ötletének megszületését az Anonimnij International egyik tagja.

Az első tweet után fél órával az orosz elnök sajtótitkára, Dmitrij Peszkov ezt közölte az információs ügynökséggel: „Nagy valószínűséggel feltételezzük, hogy ez hekkertevékenység következménye." A kormányzatban megerősítették: „A miniszterelnök twitterét feltörték. A legutóbbi üzeneteknek, amelyek a mikroblogon megjelentek, nincs közük a valósághoz." A miniszterelnök sajtószolgálata eltávolított néhány tweetet, azonban a férfinak a kávézóból még valamit sikerült írnia: *„Képesek vagyunk visszamenni a 80-as évekbe. Ez szomorú. Hogyha a kollégáimnak a Kremlben ez a célja, akkor ezt hamar el fogják érni. [...] Az oroszok nem kötelesek szenvedni amiatt, hogy az ország legfelsőbb vezetésének gondot jelent, ha a józan gondolkodás nyilvánul meg."*

Búcsúzóul visszatweetelt az Anonimnij International accountjára, az @bOltaira: *„A cirkusz a bohócok szétszéledésével ért véget. Tiltsák be az elektromosságot."*

„Alkotó technikus" – így nevezik az Anonimnij Internationalben azt, aki Medvegyev twitterére írt, és aki annyi tweetet tudott írni, amennyit csak szükségesnek látott:

ezeket a közösségi hálóról senki sem tudta eltávolítani. A sajtószolgálatnak, hogy gátat vessen a történéseknek, meg kellett kérnie a szolgáltatás adminját, hogy blokkolja Medvegyev fiókját. Egy órával később a férfi ezt írta chaten a kollégáinak: *„Unalmas megdönteni a kormányt"*, majd bezárta a notebookját, és kiment a kávézóból.

* * *

A Saltaj-Boltaj az orosz kiberellenállás utolsó sikeres projektje. Először 2013. december 31-én adtak hírt magukról, amikor publikálták Vlagyimir Putyin újévi köszöntőszövegét néhány órával az előtt, hogy az megjelent volna az éterben. A következő tizenkét hónapban az Anonimnij International főként olyan levelezéseket posztolt, amelyet a különböző rendű és rangú orosz politikusok e-mailjéről vagy telefonjáról töltött le. A posztok végén ez a jelmondatuk állt: *„Mindig Önökkel, még akkor is, amikor ezt Önök nem is gyanítják."*

2014 tavaszán a Saltaj elárasztotta a világhálót egy moszkvai találkozó forgatókönyvével, amely támogatta a Krím Oroszországhoz csatolását, továbbá egy arról szóló dokumentummal, hogy az elnöki adminisztráció referendumot készített elő a félsziget hovatartozásáról. Nyilvánossá tette ezen kívül Igor Sztrelkov-Girkinnek,* az FSZB egy volt ügynökének a privát levelezését, aki akkoriban a híveivel együtt éppen hadműveletet hajtott végre Ukrajna keleti részén. Arról szóló dokumentumokat is közzétettek,[329] hogy Jevgenyij Prigozsin cége, a Konkord az Internetvizsgáló Ügynökségen keresztül miként felügyelte a Kreml „internettrolljait".

Igor Oszadcsij (őt úgy emlegették az Internetvizsgáló

* Igor Vszevolodovics Girkin néven született Igor Ivanovics Sztrelkov, egykori katonatiszt, aki meghatározó szerepet játszott azokban a 2014-es krími és donyecki hadműveletekben, amelyekben a moszkvai kormány hivatalosan mindmáig tagadja részvételét.



Ügynökség levelezésében, mint a *Fordító* nevű projekt vezetőjét, aki a hírek külföldi médiában való elhelyezéséért felel) a publikációkban saját személyes adatait fedezte fel, és bírósághoz fordult. A Roszkomnadzor képviselője közölte: „A bíróság határozatot hozott arról, hogy az információkat el kell távolítani, de a tartalomszolgáltató nem reagált az értesítéseinkre, ezért a felügyelet kiadott egy utasítást a szolgáltatónak a blog blokkolásáról." 2014. július 27-én a bOltai.org erőforrásaihoz való hozzáférést Oroszországból a Roszkomnadzor követelésének megfelelően blokkolták, és hamarosan ugyanez a sors várt a csoport fő Twitter-csatornájára is. Most a Saltaj-Boltaj az Oroszországi Föderációban csak a VPN-en vagy a tükörweboldalon[330] keresztül érhető el, a tartalék @bOltai2 Twitter-oldal lemásolt minden bejegyzést a blokkoltról – egészen a viszonttweetekig.

A blokkolás előtt pár nappal az internetaktivisták Arkagyij Dvorkovics miniszterelnök-helyettes hivatalos levelezését posztolták ki:[331] ő volt az, aki azt követelte, hogy módosítsák a 2015-2017 évek büdzséjét, máskülönben „nem biztosítható a programtervben vázolt feladatok megoldása". Egy hónap múlva az Anonimnij International Dmitrij Medvegyev három postafiókjáról adott információt,[332] és nyilvánossá tette az Egységes Oroszország Párt küldöttének, Robert Schlegelnek a „trollok" elleni támadás megszervezéséről szóló levelezését a legnagyobb külföldi médiumok honlapjain (a *The New York Times*on, a CNN-en, a BBC-n, a USA *Today*en és a *The Huffington Post*on).

2014 őszén a Saltaj a kormányzattal kapcsolatban álló Moszkovszkije Informacionnije Teknologii nevű cég elektronikus levelezésével árasztotta el[333] az orosz médiát (a *Komszomolszkaja Pravdát*, az *Izvesztyiját*, a *Rosszijszkaja Gazetát*, a *Lityeraturnaja Gazetát*, a *Regnum*ot) – ily módon a tisztviselők tulajdonképpen a sajtóban tettek közzé törvénycikkeket. Szintén közölték Igor Suvalov miniszterelnök-helyettes tanácsadójának hivatalos levelezését.[334] 2014 decemberében az Anonimnij International egy fotót posztolt, amelyen a

Mieink mozgalom korábbi sajtótitkára, Krisztina Potupcsik feltételezhetően az elnöki adminisztráció dolgozószobájában ül, egy pénzzel kitömött táskával.[335]

Két hét múlva az aktivisták Timur Prokopenkónak, az elnöki adminisztráció belpolitikai igazgatóhelyettesének a hivatalos levelezését hozták nyilvánosságra. Prokopenko e-mailekben taglalta az Alekszej Navalnij elleni támadáshoz megrendelt anyagokat,[336] és sms-ben érintkezett Alekszej Goreszlavszkijjal, aki akkor a nagy orosz internetes holding, a Rambler & Co külső kommunikációjáért felelős igazgatóhelyettesként dolgozott (ebbe a holdingba vonták be az ország két legnépszerűbb internetes lapját, a Lenta.ru-t, ahol akkoriban dolgoztam, és a Gazeta.ru-t).

– *Ide hallgass, ők egyáltalán nem figyelnek rád?* – érdeklődött Prokopenko.

– *Én számukra nem vezető vagyok, ez egy. Nagyon erősen ajánlhatom, mit csináljanak, de bárkit kirúgni és pénzbüntetést kiszabni nem tudok. A Gazetánál hallgatnak rám, de a szerkesztőség még élvezkedik, marihuánás cigaretta is van. A Lentánál a pozícióm mindenre kiterjed, Galja* [Timcsenko, a kiadó főszerkesztője] *utalt arra, hogy nála ez „standard", és ő ezt teljesíteni fogja. A kérdés fel van téve a részvényesek számára. Azt csinálom, amit tudok.*

Az üzenetváltás után húsz nappal a Lenta.ru főszerkesztőjét, Galina Timcsenkót elbocsátották, őt követve távozott szinte az egész kiadói csapat – beleértve engem is.

Prokopenko üzenetei és levelei alapján teljesen világossá vált, hogyan működik Oroszország elnöki adminisztrációjának belpolitikai hivatala. Például az elnöki hivatal munkatársai az ellenzéki Alekszej Navalnij minden lépését szemmel tartották az interneten, feljegyzéseket készítettek a független kiadványok szerkesztőségi politikájáról, tanulmányozták a tweeteket és a közösségi hálón megjelenő mémeket. Prokopenko mindennap többoldalas jelentéseket kapott a legfontosabb témákról, amelyeket a Twitteren, a Facebookon és a Zsivoj Zsurnalon tárgyaltak meg. Minden beszámoló ajánlással végződött, hogy milyen megvilágításba kellene helyezni ezeket a témákat. Például ily módon: *„Azzal a mozgáskorlátozott nővel kapcsolatos témát, aki egy garázsban lakik a hivatalnokok tétlensége miatt, magára vállalhatná az ONF* [az Összorosz Népi Front, amelyet 2011-ben az ellenzékkel szembeni ellenállás és Vlagyimir Putyin támogatása érdekében hoztak létre]*, biztosítva a nő számára a feltétlenül szükséges információs és jogi támogatást lakhatási problémái megoldásához és a vele szemben vétkes hivatalnokok megbüntetését."*

Prokopenko többször érintkezett a Roszkomnadzor vezetésével a kellemetlen honlapok blokkolásával kapcsolatban. A hivatal fejével, Zsarovval tárgyalt arról, hogyan blokkolják az ukrán nacionalisták csoportját a VKontaktén: Zsarov sajnálkozott, hogy a VKontakte akkori vezetője, Pavel Durov „játssza a hülyét" és „nem enged utat több blokkolásnak". Prokopenko felajánlotta, hogy együttműködik az államügyészséggel és „leszedik" (nem sokkal később Durov el is hagyta Oroszországot, és felhagyott a VKontakte vezetésével).* Megtárgyalták a „Szibéria föderalizációjáért" szóló tüntetés** BBC-s közlését is. A Roszkomnadzor munkatársa ekkor felajánlotta, hogy ezt is blokkolják, és ezt írta: „A szigetről származó emberek elszemtelenedtek." Prokopenko figyelmeztetett, hogy „ott (Nagy-Britanniában) a *Russia Today* kárt szenvedhet". Végül a Roszkomnadzor nem nyúlt hozzá a BBC-hez. A társa-

* Durov kénytelen volt eladni az „orosz Facebook"-ot egy államközeli cégnek, később azonban létrehozta a Telegram nevű messenger-alkalmazást. – *A szerk.*

** 2014 augusztusában tüntetést szerveztek Novoszibirszkben Szibéria föderalizációjáért *Elég Moszkva etetéséből!* címmel. Nem Oroszország területi egységét kívánták megkérdőjelezni, kiszakadni belőle, csak jóval nagyobb helyi beleszólást kívántak a régió életébe a helyiek. Az olaj- és gázbevételek elosztása is központi témája volt a követeléseknek. A szervezőcsoport VKontakte-oldalát a legfőbb ügyész rendelkezése alapján blokkolták. Novoszibirszk polgármesteri hivatala betiltotta a tüntetést. – A ford.

ság orosz részlegének vezetését a hivatal 2019 elején kezdte ellenőrizni, válaszként a brit kormány érdeklődésére a *Russia Today* ottani tevékenysége iránt.

Prokopenko egy FSZB-s tábornok fia, a katonai egyetem és az elnök alá tartozó Közszolgálati Akadémia végzett hallgatója. Egykor az ITAR-TASZSZ állami hírügynökség különtudósítójaként dolgozott (olykor ezek az állások a hírszerzés elfedésére szolgálnak), azután pedig az állami dumában és a Kreml-barát ifjúsági mozgalmakban tevékenykedett. Az elnöki adminisztrációba Vjacseszlav Vologyin vitte be, aki a tömeges tiltakozások után a belpolitika felelőse lett az államfői hivatalban.

Prokopenko egész 2010-es évek eleji tevékenysége emlékeztet Howard Huntéra, aki az 1970-es években az Egyesült Államokban Nixon elnöki adminisztrációjában dolgozott, és a Watergate-botrány egyik főszereplőjévé vált. Hunt végül majdnem három évet ült. Prokopenko levelezését senki még csak meg sem vizsgálta, habár ebből az következne, hogy a Kreml cenzúrát alkalmaz, és üldözi az ellenzéket. Prokopenko most is az elnöki adminisztrációban dolgozik.

Az interjúban, amit (kriptochaten) az Anonimnij International sajtótitkárának adtak, a Saltaj-Boltaj megerősítette,[337] hogy azért közölnek kompromittáló anyagokat, mert „nincs ínyükre az internet szabadságának korlátozása, az agresszív külpolitika", valamint nem tetszenek nekik az orosz politika egyéb sajátosságai sem, mint például a tisztességtelen választások, a kis- és középvállalkozások működését szabályozó előnytelen feltételek. Az Anonimnij International „a világ jobbá tételét hirdette meg[338] céljaként, ami alatt például a társadalom nagyobb szabadságát és informálását értik".

A csoport egy tagja a *Watchmen: Az őrzők* című filmből idézett:[339] „Ezt azért tesszük, mert szükséges. Ha az ember csak egyszer is meglátja a társadalom sötét oldalát, többé soha ne fordítson neki hátat."

* * *



A csoport twitterén megtaláltam az e-mail-címüket és írtam nekik, találkozót ajánlva. „Amennyire ki tudtam venni, nem Oroszországban és nem is Moszkvában tartózkodtok. Vagy valaki mégis itt van?" – kérdeztem. Még aznap válaszoltak: „Kicsit tévedésben vagy. ☺ MI NEM találkozunk Moszkvában vagy Oroszország más városaiban. Gyakorlatilag a csapat minden tagja az Oroszországi Föderáció állampolgára, és nagyrészt az Oroszországi Föderáció területén lakik. De képviselőink kizárólag az Oroszországi Föderáció határain kívül találkoznak. A következő hónapokban ezeken helyeken: Isztambulban, Bejrútban, Bangkokban, Kijevben. A pontos idő és hely ezekben a városokban további egyeztetés kérdése." Erre azt kértem, hogy amikor nekik alkalmas, találkozzunk Isztambulban.

Két héttel később ezt írták: „Isztambulból távozott az emberünk. Lehetséges, hogy nem megy oda vissza többé. (Vannak embereink még Bejrútban, Kijevben, Bangkokban.)" Egy újabb hét elteltével kiderült, hogy a találkozó egyedül Délkelet-Ázsiában lehetséges, leginkább Bangkokban. Azt válaszoltam, hogy az túlságosan messze van. „Ellenben ott meleg van, olcsó a pia és a nők. ☺ Vicc volt ☺ – válaszolták. – Ennek ellenére felmelegszünk ☺ Különben is, közelebb hideg van." „Na, jól van, a hideg felélénkít. Lehetne közelebb?" – írtam én.

– De ha komolyra fordítjuk a szót, vannak még okai [hogy ne találkozzunk közelebb].

– Azt gondoljátok, hogy követtek benneteket? – kérdeztem én.

– Azt gondoljuk, hogy nem követtek. ☺ Mi nem hagyunk sok nyomot magunk után. De nem félünk semmitől, mert tisztességesek vagyunk. ☺ Ha akarsz, hiszel, ha nem akarsz, nem hiszel a tisztán családi indítékokban. ☺ Mindannyian emberek vagyunk, emberek. ☺

2014 decemberében megírtam nekik, hogy szabadságra Hongkongba készülök, és onnan át tudnék utazni Bangkokba. Beleegyeztek, és azt tanácsolták, az etióp légitársa-

sággal repüljek, mert „ott rendkívül elbűvölőek a stewardessek, etiópok, tehát fekete bőrűek és kék szeműek". Voltak egyéb tanácsaik is: „Hongkongban karácsonykor és annak előestéjén [a katolikusok] hemzsegnek a központban, hogy még a gyalogosok se nagyon tudnak bemenni. Ne csodálkozz, ha 26-án este azt látod, hogy a belvárosban a gyalogosokat rendőrök irányítják, hogy kikerüljenek bizonyos utcákat. Én csodálkoztam, amikor először ilyet láttam, mert nem értettem az okát. És ha még nem foglaltál szállást, akkor igyekezz. Az árak Hongkongban ilyenkor rendszerint nagyon magasak."

* * *

Amikor megérkeztem Bangkokba, vettem egy SIM-kártyát, és írtam egy sms-t a megadott számra. A hotelben várakoztam. Pár óra múlva telefonáltak, és azt javasolták, találkozzunk a város legnépesebb körzetében, a Khao San úton. Alex Garland *A part* című regényében úgy írta le ezt a helyet, mint „a gyalogos turisták országát": „Szinte minden épület fogadóvá alakult, a távolsági telefonfülkékben légkondicionáló zümmögött, a kávéházakban a legújabb hollywoodi filmeket játszották. Az ember minden harmadik lépés után bódéba botlott, ahol csempészett videókazettákat árultak. Az út lényegében úgy működött, mint az űrhajósok légnyomás-kiegyenlítő kamrája, Thaiföld kapujában, félúton kelet és nyugat között."*

2015 januárjában a kerület nagyjából ugyanígy nézett ki. Minden második európai kézen fogva sétálgatott egy thai prostituálttal, a vidám helyi spekulánsok folyton azt sugdosták az ember fülébe: „Fű? Fű van. Szerelem? Szerelem van." Egy kicsit eltévedtem, amikor benéztem azokba az üzletekbe, amelyekben magnókazettákat árultak – köztük valamiért az 1990-es évek végének orosz popzenéjét is.

* Alex Garland: *A part*. Budapest, Park Kiadó, 1999. Losonczy Gábor fordítása.



A Saltaj emberei újra hívtak – most már egy másik számról –, és kérték, menjek oda a szomszéd utca 6-os számú házához. Amikor odamentem az épülethez, egy férfi az utca szemközti oldaláról integetett nekem.

Átfutottam az úton, mire ő fogott egy motoros riksát. A találkozóra egy mosolygós férfi érkezett szalmakalapban és könnyű nyári öltözékben, vállán átvetve egy kis táska volt a notebookjával. Ő, természetesen, nem kívánt bemutatkozni, de én elhatároztam, hogy Lewisnak hívom: a csoport tagjai úgy vélték, hogy az *Alice Csodaországban* a maga visszájára fordított logikájával pontosan leírja az orosz politika világát.*

A tuk-tuk egyszer csak elindult, nekiiramodtunk, és elkezdtünk az autók között szlalomozni. Lewis azonnal mesélni kezdett a csoport tevékenységéről, de az utcán olyan nagy volt a zaj, hogy én csak bizonyos szavakat értettem: „egyéb játékok melléktermékе", „a torony képviselői", „Prokopenko", „saját munkaterv".

Vagy tizenöt perc múlva megálltunk Bangkok központjában. Lewis átnyújtott a sofőrnek pár bankjegyet, miközben megállapította, hogy itt az utazás nagyon olcsó, és azt javasolta, menjünk le a metróba, hogy egyértelműen meggyőződhessen róla, senki sincs a nyomunkban.

*„Nemrég muszáj volt találkoznunk egy orosz újságíróval* – magyarázza. – *Nagy adatbázisunk van – ellenőriztük. Kiderült, hogy az ő postáját is megnyitották, hogy megtudják, ki ő és ki után kutakodik. Ezért a találkozást az utolsó pillanatban kénytelenek voltunk elhalasztani. Ellenőriztek téged is, de semmit se találtak nálad. Én mégis megkértem Boltajt, hogy figyelje meg, nincsenek-e a nyomunkban."*

– *Boltaj is itt van?* – kérdeztem vissza.

– *Igen, ő itt lakik. Én pedig egy napra jöttem, hogy átadjam neki a fájlokat. Amikor nálad van néhány gigabájtnyi informá-*

* Lewis Carroll az *Alice Csodaországban* szerzője. *A fordító megjegyzése.*

*ció, egyszerűbb, ha a merevlemezt személyesen adod át, mint a hálózaton keresztül. Minden információt legalább két másolatban őrzünk különböző országokban. És nincs olyan ember, aki teljes hozzáféréssel rendelkezne mindegyikhez. Boltajjal ma szerettünk volna úszni egyet a háza medencéjében, de hideg van.*

*Értsd meg, az Anonimnij International egyikünknek sem a főfoglalkozása* – folytatta Lewis. – *Nem ezzel foglalkozunk állandóan. A Saltaj-Boltaj az egyéb játékok melléktermék. IT-biztonsággal foglalkozunk és... Hogy kell ezt mondani?*

– *Veszéllyel?*

– *Igen. És IT-veszéllyel.*

– *Feltörésekkel?*

– *Nem pontos a meghatározás. A hozzáférések megszerzésével foglalkozunk. Ez nem feltétlenül a feltörés útja.*

– *De feltörés is lehet?*

– *Természetesen. De gyakoribb, hogy a hozzáférést vagy az információt más utakon szerezzük meg. Például elmész egy emberért a kávézóba, hogy megnézd, hogyan toboroz* [a klaviatúrán]. *Olykor, hogy megkapd az információt, muszáj meggyőzni. Van, hogy szép szóval, van, hogy nem, néha pénzzel, néha információval. Gyakran mennek el mellettünk projektek, amelyek szoros kapcsolatban állnak a Kremllel. A főfoglalkozásunkból mindig jön valami, ami ott nem használható. Ez az információ kerül be az Anomnij Internationalba.*

– *Sok kliensetek van?*

– *Kis klientúránk van, de az állandó. Nekünk ez elég. A tarifánk néhány tízezer dollárnál kezdődik. A felső plafonról nem fogok beszélni. Mindannyiunknak elég ez a megélhetésre és az utazásokra.*

– *Kik a megrendelőitek? Kinek adjátok el az információt?*

– *A főfoglalkozásunk révén az állami struktúráktól is és magánszemélyektől is kapunk megrendeléseket. Soha nem dolgozunk azokkal, akik kábítószer-kereskedelemmel állnak kapcsolatban. Független csapat vagyunk. Gyakran egyszerűen nem is tudunk rájönni, ki a megrendelő. Van úgy, hogy közvetítők*



*számára szerzünk információt, nem tudva, ki az eredeti megrendelő.*

Abban a pillanatban senki sem tudta, ki áll az Anonimnij International mögött. Sokan találgattak, egyesek azt gondolták, maga Timur Prokopenko, mások szerint az elnöki adminisztráció sajtófőnöke, Alekszej Gromov (mivel róla nem tettek közzé soha semmit a hekkerek), megint mások pedig azt, hogy Vlagyiszlav Szurkov.

„A legnevetségesebb, hogy a fent említettek valahogy mind ott vannak, hisz van ez az embertípus – mondta nekem az egyik belpolitikai munkatárs. – Kezdetben mindenkinél razzia volt, nyáron, például, de most nem. [...] Az egyik csoport, akkor, amikor keresték, még Londonig is eljutott, de aztán nyomuk veszett. De a legtöbben a hivatalra gondolnak.* A srácoknál rengeteg információ van, és azokat senki sem tudja elégetni."

– *Tudjuk, hogy keresnek minket* – folytatta Lewis. – *Májustól egy tábornok van ránk állítva, aki kezdetben a belügyminisztériumban, aztán az FSZB-nél és az FSZO-nál dolgozott. Van egy tucat sms-ünk Prokopenkótól, amelyekben ez a tábornok kijelenti, hogy lám-lám, már közel vagyunk, majdhogynem összejön az akció, aha. Nyáron közvetítőkön keresztül jöttek hozzánk olyan emberek, akik azt kérték, törjük fel az Anonimnij International fiókját, természetesen nem tudta, hogy mi ők vagyunk. És hogy a fő célunknak nem a feltörést tűztük ki, hanem a résztvevők személyének végső tisztázását. Borsos árat kértünk, százezer dollárt. Ezt visszautasították. Bár én nem nagyon értem, miért, ez az ár nem is olyan magas.*

(Már a találkozónk után, 2015-ben, a Saltaj-Boltaj nemcsak posztolni kezdte a levelezések archívumait, hanem árusítani is internetes tőzsdéken. A Joker.buzz weboldalán a csoport 1000 *bitcoin* értékben kötött ügyleteket, ami körülbelül kétszázhetvenötezer dollár volt az akkori árfolyam szerint, 2019 februárjában pedig 3,4 millió dollár.)

* Azaz az FSZB-re. – *A szerző megjegyzése.*

*– Ezt azt jelenti, hogy a főfoglalkozásotok a vádló bizonyítékok összegyűjtése?*

*– Nem. Mi a valóság megváltoztatásával foglalkozunk. Olykor ehhez a munkához nem pusztán az információk összegyűjtésére van szükség.*

*– Ez egyáltalán nem világos.*

*– O. Henrynek van egy elbeszélése – a címére nem emlékszem – arról, hogy egy fiatalember sehogy se tud egy lánynak ajánlatot tenni, mert az nagyon elfoglalt.* De éppen úgy adódik, hogy a fiatalember ezzel a lánnyal dugóba kerül, illetve történnek még bizonyos események, és szerelmet vall neki. Ezt követően az apjához valaki egy pénzügyi kimutatással érkezik: hogy mennyit is kell fizetni a taxisoknak, meg a rendőröknek, meg mindenkinek, aki ott volt a dugóban. Mi nagyjából ugyanezzel foglalkozunk. Hogy egy ember ott találja magát, vagy ne találja ott magát egy meghatározott helyen, és hogy az információk abban a bizonyos pillanatban legyenek közzétéve.*

*– Mondj egy példát a valóság megváltoztatására.*

*– A főfoglalkozásunk terén elértük egy kormányzó elbocsátását. Letettünk a megfelelő ember asztalára egy mappát. Nem fogom a nevét megmondani.*

*– Ki dönt a fáljok publikálásáról?*

*– Mindent együtt beszélünk meg. De én egyedül is tudok dönteni a publikálásról.*

*– Mi vált ki leginkább vitákat?*

*– Girkin, természetesen. Boltaj nálunk a legradikálisabb, aki ezt mondta: „Ki kell fektetni azt a szemetet." Saltaj fordítva. De a technikusoknak kell a hírverést megoldaniuk. Prokopenko viszont nem váltott ki vitákat. Az, hogy akkor mi kiposztoljuk Potupcsik fotóját* [pénzért], *Prokop számára világos volt. Rögtön felfogta, hogy nálunk van. Általában csak a társadalmilag hasznos információkat tesszük közzé. Soha nem közlünk személyeset.*

* Az *Arany és szerelem* című elbeszélésről van szó. – *A szerző megjegyzése.*



*– Ez azt jelenti, hogy tiltva csak a személyes van?*

*– Soha nem fogunk államtitkot publikálni.*

*– Ha a Snowden-fájlokhoz hasonló adatok lettek volna nálatok, kitettétek volna?*

*– Valószínűleg nem. Nem mindent kell kiadni.*

*– És hogyha a fájlok államellenes bűncselekményről szólnak?*

*– Akkor közzétesszük.*

*– De Snowden államellenes bűncselekményekről tett közzé fájlokat.*

*– Az, amit ő kitett, minden szakember számára már nagyon régen ismert volt.*

*– Hogyan kerülnek hozzátok fájlok a feltörésen kívül? Kik a hírforrások?*

*– Az elnöki adminisztráció néhány munkatársának tetszik, hogy részese a harcnak. Amikor Moszkvában vagyok, néhánynyal találkozom egy ebéd erejéig, én is ellátom őket információval, és ők is ellátnak engem információval. Alapvetően a hírforrások hosszú évek óta az ismerőseim. Néhányan a főfoglalkozásunk miatt látnak el bennünket információval, nem tudva, hogy mi az Anonimnij International vagyunk. Ismeretlen kezdeményezőkkel nem dolgozunk. Nagyon bonyolult az ellenőrzésük.*

*– Kiről fognak szólni a következő kompromittáló anyagok?*

*– Nálunk van nagyjából két terrabájtnyi fájl. Van sok fájl olyan emberekről, akik közel állnak VVP-hez.* Prokopenkóról eddig csak a tíz százalékot közöltük. Van negyvenezer sms-ünk, ott van a liberális újságírókkal folytatott hatalmas levelezés, például. Tudjuk, hogy a leggyakoribb verzió, hogy Gromovon dolgozunk, de az, hogy semmit se publikáltak róla, nem jelenti azt, hogy semmit se fogunk róla közzétenni.*

*– Ez azt jelenti, hogy lesz?*

*– Azt mondtam, nem jelenti azt, hogy semmi sem lesz róla publikálva.*

* Azaz Vlagyimir Vlagyimirovics Putyinhoz. – *A szerző megjegyzése.*

*– Miért fordítotok akkora figyelmet Prokopenkóra?*

*– Prokopenkót több mint két éve szemmel tartjuk. Most vált pozíciót.* Számunkra fontos volt, hogy végre megmutassuk, mivel is foglalkozott az utóbbi időben.*

Lewis kivette a notebookot a táskájából, kutakodott egy ideig a fájlok között, majd felém fordította a képernyőt. A képernyőn Dmitrij Medvegyev volt, a dolgozószobája karosszékében ült, az asztalán pedig rengeteg színes mappa hevert. „Íme, itt vannak az asztalon a mappák, bennük a legérdekesebb dolgok, amelyekhez nagy nehezen hozzájutottunk" – mondta Lewis.

Szavai szerint az Anonimnij International publikációi után az elnöki adminisztrációban minden egyes munkatársnak megtiltották, hogy a magánlevelezését használja. Most mindenkinek védett fiókja van, amelyre csak meghatározott IP-vel és meghatározott számítógépen keresztül lehet belépni, de, magyarázta Lewis, a miniszterelnök-helyettes tanácsadójánál magasabb pozícióban lévő munkatársak ezeket az előírásokat nem tartják be: „Nem fog odamenni egy FSZB-s Dvorkovicshoz, és nem fogja neki ezt mondani: Na, gyerünk, gyerünk már, kapcsold ki!"

Kiléptünk a metróból az utcára.

*– Amikor megláttalak azzal a hátizsákkal és a fejhallgatóval, azt gondoltam, könnyen készíthetnél rólam hangfelvételt, le is tudsz fotózni* – mondta Lewis. *– És akár holnap közzéteheted a fényképemet.*

*– És akkor mit fogsz csinálni? Hogyha közlöm.*

*– Többet nem megyek Oroszországba. Ellenben a családod mellé teszek egy pipát, és ha alkalom adódik rá, aláteszek nekik. Nos? Prokopenko vajon killereket küld? Bár... Hogyan lehetne engem megtalálni Ázsiában? Lehetetlen.*

Azt kérdeztem, le lehet-e fényképezni a notebookját

* Az információs politika helyett 2014 decemberétől a szövetségi szintű pártok és választások felügyeletét végezte az elnöki adminisztrációban. – *A szerző megjegyzése.*



vagy a sapkáját. Azt megtiltotta, hogy a számítógépét fotózzam, a sapkáját azonban felakasztotta egy kerítésre, úgy, hogy ne legyen semmilyen cégtábla a háttérben. „Akkor nagyon könnyű lenne idejönni és fizetni a térfigyelő kamerák felvételeiért – magyarázta Lewis, miközben vett egy ananászlevet az utcán. Előszedett a táskájából egy kis üveg gint és felhörpintette, majd előszedett a zsebéből egy eldobható telefont, amelyet a velem való kapcsolattartásra használt. Egy zsebkendővel letörölte az ujjlenyomatokat, kivette a SIM-kártyát és az akkumulátort, ezeket különböző szemeteskukákba dobta, és vonattal a repülőtérre sietett.

* * *

2017. november 10-én a Pulkovo repülőtéren, még mielőtt Minszkbe indult volna, letartóztatták Vlagyimir Anyikejev orosz állampolgárt a barátnőjével együtt. Három nap múlva elengedték.

Csak ezután derült ki, hogy Anyikejev kapcsolatban állt a Saltaj-Boltajjal, és hogy én éppen vele találkoztam Bangkokban.

*„Lehet, hogy maga is találkozott már olyan esettel, amikor valakit baleset ért, agyrázkódást szenved el, s utána valahogy olyan visszafogottá, különössé válik – emlékezett vissza később a csoport egy másik munkatársa. – Nagyjából ugyanígy változott meg* [a letartóztatása után] *Anyikejev is. Kissé bizalmatlan voltam, megkértem, térjen be a Zsan-Zsakba a Tagankán, és csináljon egy szelfit a szórakozóhely cégérével a háttérben. Megtette. Elküldte a szelfit, aztán azt mondtam, hogy küldjön egy éles képet, mire ő küldött egy éles fotót az ötös asztalról: az asztalon ott volt a pincér családneve, és két kávé. Telefonáltam a Zsan-Zsakba, ezt a pincért kértem, és azt kérdeztem: »Éppen most volt önnél az ötös asztalnál rendelés tíz perccel ezelőtt. Mondja, ott egy férfi volt, vagy ketten voltak?«"*

A pincér azt válaszolta, hogy a férfi egyedül volt, de interjúalanyom ekkor továbbra is kételkedett: hogy lehet meginni két csésze kávét tíz perc alatt? Szavai szerint

Anyikejev beismerte, hogy a titkosszolgálatok tárgyaltak vele a Saltaj-Boltaj tevékenységéről, de hangoztatta: „minden kérdés alapjában véve meg van oldva, bizonyos részletek el fognak rendeződni." „Anyikejev azt mondta, hogy a velük folytatott tárgyalások révén, amelyek segítettek megoldani a kérdést, a projekt tovább működhet, de minden résztvevőjének muszáj Oroszországba utaznia és ellenőrzés alá kerülnie, a biztonságuk érdekében is" – meséli a Saltaj-Boltaj egyik tagja. Végül Anyikejev rávette egy üzlettársát, hogy utazzon Oroszországba – ezt követően az FSZB munkatársai azonnal letartóztatták magát Anyikejevet is, a vele érkezőt is, és még néhány Saltaj-tagot.

2017 márciusában a lakásra, amelyben tizennyolc éves koromig éltem, s amelyben a rokonaim azóta is laknak, kiszálltak az FSZB munkatársai. Engem kerestek, és otthagytak egy értesítést arról, hogy beszélgetésre hívnak.

Mivel nem tudtam, mire számítsak, másnap elmentem abba a városrészbe, ahol születtem. Általában ott megnyugszom, de most teljesen máshogy éreztem magam. Az ismerős udvaron figyelmesen nézegettem a járókelőket, gondosan szemügyre véve egy férfit. Sötét öltönyt viselt, és nem az ő mérete volt. De láttam néhány nőt is, akik a szokott módon a bejárat előtti kis padon beszélgettek.

Egy nappal később átmentem Lefortovóba, az FSZB kiemelt vizsgálati intézetébe, amely az azonos nevű börtönnel egyazon épületben található. Ez az épület egy hétemeletes lakóház mögött helyezkedik el egy játszótér szomszédságában, mellette van néhány kávézó, amelyekben általában a vádlottak rokonai találkoznak az ügyvédekkel.

Tudtam, hogy a portán le kell majd adnom a telefont, ezért inkább a kocsiban hagytam: azt gondoltam, ha az FSZB kezében hagynám, az valójában azt jelentené, beleegyezem a lehallgatásba és a feltörésbe. A portához egy nyomozó érkezett, aki Jasztrebovként mutatkozott be. Felvezetett. Nélküle visszafelé nem mehettem ki: a folyosók alkotta labirintus vargabetűt írt le, a lépcsők jobbra és balra



is vezettek, a folyosók az emeletek között kezdődtek, és nagyon messzire nyúltak.

A nyomozó dolgozószobája mellett a falon fémszerkezet meredezett a ráerősített bilincsekkel. „A vallatásokhoz?" – kérdeztem. „Nos, igen" – suttogta Jasztrebov. A dolgozószobában a kopott linóleumon állt egy asztal, megrakva papírokkal, és egy nagy, szürke, fémből készült széf, az ajtón pedig egy naptár lógott Feliksz Dzerzsinszkij portréjával.

Jasztrebov közölte, hogy nem engedik meg neki az internethasználatot, ezért nem olvasta a Saltaj-Boltajjal való találkozómról szóló riportomat. Hogy megkapja a hozzáférést a szöveghez, a nyomozónak fel kell iratkoznia egy listára, várnia kell a sorára, hogy megkapja a kulcsot, és csak ezután mehet be abba a szobába, ahol az a számítógép van, amely rá van kötve az internetre. A telefonokat a nyomozók, ugyanúgy, mint a látogatók, az épület bejáratánál leadják.

Jasztrebov az Anyikejevvel való bangkoki találkozómról kérdezősködött, és megkért, a saját szavaimmal mondjam el az egész riportot. Néhány óra múlva a nyomozó azt ajánlotta, menjünk ki dohányozni. Átmentünk az emeleten, és megálltunk az egyik folyosó mellett, amelyet rács zárt le. „Itt kezdődik a börtön, ide jobb soha nem bekerülni" – mondta a nyomozó. „Aha" – bólintottam, és elszívtam a cigarettámat.

* * *

Anyikejevet néhány feltöréssel vádolták. Az ügyét nyilvánosan vizsgálták, bár általában az ilyen ülések zárt eljárásban zajlanak.

Amíg Anyikejev tárgyalása tartott, a csoport egyik szabadon maradt tagja – ő az, aki magát Saltajnak hívja – a médiához fordult azzal az ajánlattal, hogy interjút ad. Rigában találkozott a Meduzával, aztán pedig Tallinnban a Dozsggyal,[340] ahol úgy döntött, politikai menedéket kér. Az újságírókkal láthatóan abban a reményben beszélgetett, hogy ez meggyorsítja ezt a folyamatot.

Saltajt Alekszandr Glazasztikovnak hívták. Közölte: a csoport többi tagját épp most fogták el, takargatnivalója nincs, mivel a titkosszolgálatok minden bizonnyal tudnak róla mindent. Glazasztikov elmondta, hogy az Anonimnij International leendő tagjai 2004-ben ismerkedtek meg egymással Dmitrij Grizlov erotikus estjein. Ő Borisz Grizlov politikus fia, aki sokáig az Egységes Oroszország Pártot és az állami dumát is vezette. A parti után időnként kapcsolatban maradtak, de a Saltaj-Boltajt csak 2013-ban gondolták ki. Anyikejev addigra már körülbelül tíz éve foglalkozott „fekete piárral", a kormányzati körből és az akörül forgolódókból szerzett ismerősöket, akik elárasztották bennfentes információkkal.

Az első dokumentumok egyikét a Saltaj-Boltaj azután kapta, hogy a számára ismerős hekkerek tömegesen küldtek szét adathalász leveleket orosz hivatalnokok körében. Ezután Saltaj megszerezte az ellenőrzést néhány postafiók felett – volt olyan hivatalnok, aki még azt sem tudta meg, hogy feltörték.

„A szervezetet politikai célból hozták létre, hogy titkokat tárjanak fel azokról, akik Oroszország kormányával és az elnöki adminisztrációval kapcsolatban állnak" – magyarázta Glazasztikov. Ő válogatott volna a feltárandó titkok közül, például nem akarta, hogy titkosszolgálatok érintő dokumentumokat szivárogtassanak. A kollégái másképp gondolták. 2015 augusztusában a csoport közzétette az ellenhírszerzés nyílt levelét. Ebben azt fejtegették, hogy sikerült feltörniük a védelmi minisztérium magas rangú munkatársainak postafiókját. „Sajnálattal vettük tudomásul az Oroszországi Föderáció védelmi minisztérium egy sor alosztálya munkatársainak inkompetenciáját információbiztonság terén, konkrétabban fogalmazva, bűnös hanyagságukat – nyilatkozta a Saltaj-Boltaj. – A Yandex.ru, a Mail.ru és az amerikai mail.com típusú, ingyenes postaszolgáltatásokon keresztül továbbították a nem rejtjelezett szolgálati dokumentumokat, gyakran olyan titkos információknak állítva be ezeket, amelyek az Oroszországi Föderáció védelmi képességeivel függnek össze." A hivatalnokok levelezéseiben ott szerepeltek a védelmi minisztérium más alosztályainak szolgálati szervereire vonatkozó jelszavak is.



Glazasztikov biztos benne, hogy pontosan ezután kezdtek aktívan vadászni rájuk. Az ismerősök rövidesen közölték a hekkerekkel, hogy a GRU tudja a valódi nevüket. Az FSZB ezt követően léphetett kapcsolatba Anyikejevvel és találkozott vele Moszkvában. A csoportnak nyugodt jövőt ígértek azzal a feltétellel, hogy egyszer majd a Saltajon keresztül publikálnak saját információkat. Glazasztikov úgy gondolja, hogy Anyikejevvel Szergej Mihajlov lépett kapcsolatba, aki akkor az FSZB CIB-nél dolgozott, és a hekkereket felügyelte. Mihajlovot röviddel Anyikejev letartóztatása után őrizetbe vették, de „Lewis" ügyvédje azt hangoztatta, az FSZB munkatársát érintő vád semmilyen összefüggésben nincs a Saltaj-Boltajjal.

Anyikejevet végül két év börtönre ítélték, a Saltaj más tagjait pedig háromra. Glazasztikov megkapta a menedékjogot, és Észtországban maradt. Azok az archívumok, amelyeket a csoport tett közzé, most is az egyik legfontosabb információforrásnak számítanak ahhoz, hogy valós képet kapjunk arról, hogyan épül fel Oroszország belpolitikája.

Anyikejev 2018 augusztusában szabadult, később azt közölte, hogy ezután a kibervédelem biztosításával fog foglalkozni. Bizonyosan bőven lesz munkája.

# Köszönetnyilvánítás

Az *Orosz hekkerek* soha nem jöhetett volna létre a barátaim támogatása nélkül:

– Elnara Jalaltdinova <3; Jurij Bolotov és Kirill Demcsenko nélkül, akik folyton kérdezgették, mikor írom már meg végre ezt a kis könyvet.

– Ivan Kolpakov nélkül, aki a *Meduza* egyik alapítója és főszerkesztője, és akivel elhatároztuk, hogy csinálunk némi hírverést e könyv köré, és aki megengedte, hogy hosszú időre szabadságra menjek.

– A *Meduza* különtudósítói részlegének 2016 és 2019 közötti szerkesztője, Alekszandr Gorbacsov nélkül, aki a legfontosabb beszélgetőpartnerem volt a szövegekről, egyúttal az az ember, akivel mindennap vitatkoztunk is ezekkel kapcsolatban: ő az, aki ráadásul zseniálisan meg is szerkesztette ezt a könyvet.

Köszönet a Progressznek és a Starlite-nak a kávéért és a wifiért.

Ezenkívül: nem tudtam volna megírni az *Orosz hekkereket* a washingotni Kennan Institute támogatása nélkül, amely időt adott a kutatásokra.

# Fogalomtár

ADATCSEREKÖZPONT: Az adatok váltási központja az internetszolgáltatón keresztül. Ezeket az adatkapcsolatok sebességének az optimalizálása miatt is alkalmazzák.

A NULLADIK NAPI TÁMADHATÓSÁG: Sérülékenység, hiba a programban, amely ismeretlen a gyártó számára.

APT *(= Advanced Persistent Threat):* Olyan támadás, ami sokáig, akár évekig rejtve marad, nem a gyors haszonszerzés a cél, hanem a minél mélyebb beépülés a rendszerbe, minél több információ összegyűjtése, lassan, feltűnésmentesen, nyom nélkül.

BITCOIN: Nyílt forráskódú digitális fizetőeszköz. Az elnevezés vonatkozik továbbá a fizetőeszközt kezelő nyílt forráskódú szoftverre és az azzal létrehozott elosztói hálózatra is.

BOT: 1. Olyan automatizált alkalmazások/rendszerek, amelyek folyamatosan keresnek sérülékeny eszközöket. 2. Botnet értelemben: sok megfertőzött gépből álló, a támadó által irányított hálózat, amit támadásra használ (ezen keresztül rejti el a saját kilétét, illetve így lesz elég nagy sávszélessége egy DDoS-támadáshoz). 3. Utalhat a trollgyárak munkatársaira is.

BOTNET: lásd BOT.

DUMP: A bank- és hitelkártyák ellopott másolatainak adatbázisa.

DDoS-TÁMADÁS *(= Distributed Denial Of Service):* Elosztott túlterheléses támadás. Egy szolgáltatást nagyon sok különböző gépről egyszerre „használnak" a támadók, ezért a valódi legitim kéréseket már nem tudja kiszolgálni a rendszer. A kivitelezése botnettel történhet, amit saját céljaira, például: támadás, BITCOINbányászat, rejtőzködés használ.

EXPLOIT: Egy olyan program/módszer, amellyel egy másik programban lévő sérülékenységet (hibát) ténylegesen ki tudunk használni a saját céljainkra. Egy hibánál három szint lehetséges: 1. *Risk (azaz kockázatos)*, amikor teljesen általánosságban van valószínűsége annak, hogy hibás a program, és az mennyire súlyos. 2. *Vulnerability (sérülékeny)*, amikor ténylegesen van egy hiba, például egy adat beküldése után lefagy a program (tipikusan a PoC, azaz a *Proof of Concept* publikálása). 3. *Exploit* szint: amikor ezen hibán keresztül a támadó valami neki hasznos dolgot tud csinálni (nemcsak lefagyasztja a programot, hanem például tud kódot futtatni, adatot szivárogtatni stb.).

FORGALOMGENERÁTOR: Vizsgálati/támadási célra adatforgalmat generáló eszköz.

FTP: A *File Transfer Protocol* rövidítése, azaz „fájlátviteli protokoll", ami egy állományátvitelre szolgáló szabvány. FTP-azonosító és jelszó birtokában távoli szerverek tartalmához lehet hozzáférni, onnan például bizonyos állományokat beszerezni, továbbá oda állományokat feltölteni (például a saját weboldalainkat a webtárhelyünkre).

HOSTING: Többféle hosting van, itt két példa: 1. *Szerverhosting:* A számítógépek egy adatközpontba *(datacenter)* kerülnek, amely biztosítja a nagy sávszélességet, a klímát, a tápot, a hálózati redundanciát stb. Tipikusan nagyobb cégeknél fordul elő. 2. *Webhosting:* Tárhelybérlés, ahol saját weboldal hozható létre. Ők biztosítják a mentést, a sávszélességet, a redundanciát. Tipikusan kis cégek veszik igénybe.

INTERFÉSZ: Az interfész (az angol *interface* szóból) két számítógépes eszköz (a hardver és a szoftver) közötti érintkezési felület. De használják az adatkapcsolat jelölésére szoftver-szoftver között. Valamint használatos a „UI – User Interface" kifejezés is, amely azt a felületet jelenti, amelyen a felhasználó ténylegesen használja az alkalmazást.

INTERNETSZOLGÁLTATÓ: Az cég, amely lehetővé teszi az internet elérését.

IP-cím: A számítógép egyedi címe, amellyel az internetet elérhetővé (címezhetővé) teszi.

IRC (= *Internet Relay Chat*): Egy kliens-szerver alapú kommunikációt lehetővé tevő csevegőprotokoll, amelynek révén emberek tíz- vagy százezrei is cseveghetnek egyidejűleg különböző csatornákon keresztül. Amikor az ember belép, meg kell adni egy csatornát, lényegében



egy csevegőszoba nevét, ahová bekerül, és az oda küldött üzeneteket olvashatja, illetve maga is tud üzenni.

ICQ: Az angol *I Seek You*, azaz kereslek kifejezés szójátékos rövidítése. Az ezredfordulón népszerű, azóta lényegében eltűnt csevegő- és üzenetküldő program.

NEURÁLIS HÁLÓZAT: Az egyszerű processzorok egymás közötti egyesítésének rendszere, amely meg tudja tanulni a feladatmegoldást. A neurális hálózatokban minden szint kombinálódik az előző szint ismertetőjegyeivel, azaz a legbonyolultabb kombinációkat hozzák létre, amelyekről még maguk a létrehozók sem tudhatnak.

PENTESTER: Az IT-rendszerek betörésvédelmi tesztelését végző személy.

PHISHING: Másnéven adathalászat. Nagy szervezetek, például bankok, internetszolgáltatók, közösségi oldalak nevében érkező hamisított e-mailek, amelyeket valójában a támadók küldenek, hogy elcsalják az áldozatokat olyan hamis weboldalakra, ahol bejelentkezési, pénzügyi és egyéb adatokat kérnek, az adott szervezet nevében. Ha az áldozat a hamis oldalon megadja ezeket az adatokat, akkor később azokat a támadók felhasználhatják vagy eladhatják.

PGP (= *Pretty Good Privacy*): Számítógépes program, amely titkosításra és hitelesítésre egyaránt használható. A levelezés alatt a kimenő leveleket egy véletlen szimmetrikus kulccsal titkosítjuk (*session* kulcs). Ezt a szimmetrikus kulcsot titkosítjuk a címzett publikus kulcsával, és hozzácsapjuk a titkosított levélhez. A címzett megkapja, a saját privát kulcsával kibontja a szimmetrikus titkosítókulcsot, majd azzal kibontja a levelet. (A publikus és a privát kulcs mindig keresztben működik: amit az egyikkel titkosítanak, azt csak a másikkal lehet kibontani.)

PROXYSZERVER: A számítógépes hálózatok olyan komplex programja, amely közvetítőként működik a felhasználó és a ténylegesen elérni kívánt szerver között: lehetővé teszi a támadó kilétének az elrejtését a ténylegesen elérni kívánt szerver elől, mivel az csak a proxyval kommunikál, csak annak a címét ismeri. Lehet az is, hogy proxy kell egy szolgáltatás eléréséhez, ilyenek például a csak az USA-ból elérhető filmletöltő oldalak; azért használ valaki proxyt, hogy úgy tűnjön, ott van, és elérheti a szolgáltatást. VPN-t is lehet hasonló célra is használni.

TCP (= *Transmission Control Protocol*): Számítógépen futó

program és egy másik számítógépen futó másik program között egy adatfolyam megbízható, sorrendhelyes átvitelét hivatott biztosítani. Az internet gerincét alkotó TCP/IP protokollcsalád egyik fő protokollja.

TOR: Böngésző, amely elrejti a felhasználók kilétét, és lehetővé teszi a bejutást olyan weboldalakra, amelyek nem indexálhatók általános rákeresésekkel.

TRÓJAI: Olyan program, amely a felhasználó tudta nélkül végez tevékenységeket. Ezen tevékenységek lehetnek például hátsó kapu nyitása a trójai program készítője számára, vagy a számítógép vagy okostelefon erőforrásainak (pl. kamera, mikrofon) engedély nélküli használata vagy a billentyűzetleütések elmentése. A vírusokkal ellentétben általában nem többszörözi önmagát, terjedése főként egyedi támadásoknak és az emberi hiszékenységnek köszönhető.

TŰZFAL: A tűzfal egy hálózati határvédelmi eszköz, amely segít megvédeni a hálózatban található számítógépeket a hekkerektől. A tűzfal minden hálózati kérést ellenőriz, és a szabályrendszere szerint tilt vagy továbbenged.

VPN *(= Virtual Private Network)*: A legegyszerűbb módja az interneten a reális tartózkodási hely és cím elrejtésének. Virtuális magánhálózat, amely a kódolt csatorna alapján egyesíteni képes a különböző városokban és országokban lévő számítógépeket, úgy téve, mintha egyazon lokális hálózatban lennének.

WAREZ: Internetszleng-kifejezés, ami a jogvédett tartalmak jogsértő terjesztésére utal. Fő területe az internet, ahol szervezett csoportok törik fel, és teszik nyilvánossá az egyébként különböző módokon védett tartalmakat.

# Végjegyzetek


1. https://packetstechnologies.bg/bg/. A weboldal jelenleg elérhetetlen.
2. DDoS-атака 300 Гбит/с замедлила весь интернет, elérhető: https://xakep.ru/2013/03/27/60346/
3. «СМИ узнали об угрозах Касперского „мочить" конкурентов», elérhető: http://top.rbc.
4. «Сценерский лайфстайл: часть 1», elérhető: http://xakep-archive.ru/xa/090/088/1.htm
5. https://twitter.com/proxiper/status/1045631964244578304
6. «Я — создатель боевых машин-убийц!», доступно на http://xakep-archive. ru/xa/003/036/1.asp.htm
7. «Российские хак-группы: кто они?», elérhető: http://xakeparchive.ru/xa/026/044/3.asp.htm
8. «Манифест хакера», elérhető: http:// xakep-archive.ru/spec/007/053/1.html
9. «Альт F4 Ильи Гофмана», elérhető: https://www.kommersant.ru/doc/217749, illetve: https://individuumbooks.com/vtorzhenie/notes/
10. «Змеи из интернета», elérhető: http://www.mk.ru/old/article/1999/11/14/133894zmei-iz-interneta.html
11. *Dark Territory: The Secret History of Cyber War*, Fred Kaplan (Simon & Schuster, 2017)
12. «Исследование компьютерного андеграунда на постсоветском пространстве», elérhető: https://bugtraq.ru/library/ underground/research.html
13. http://www.rusdoc.ru/material/vzlom/ vybory.shtml
14. «Хакерская группа KZP — изнутри», elérhető: http://xakep-archive.ru/xa/004/032/1.asp.htm
15. Uo.
16. «Хакерская группа KZP — изнутри», elérhető: http://xakeparchive.ru/xa/004/032/2.asp.htm
17. Uo.

18. «Хакерская группа KZP — изнутри», elérhető: http://xakeparchive.ru/xa/004/032/3.asp.htm
19. http://forum.antichat.ru/
20. Antichat.ru — NoFear, elérhető: https://www.youtube.com/watch?v=ZRiGv6Q3txA&list=PLT5tHbJ PR2_opfQPmuy6pKd1C_qiWV0eD
21. https://blackbiz.club/ threads/vzlom-whatsapp-viber-instagram-facebook-uznaemvzlomaem.5098/
22. *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy,* Cathy O'Neil (Broadway Books, 2016)
23. «Андрей Станкевич стал медиаперсоной года по версии „Комсомольской правды в Санкт-Петербурге"», elérhető: http://news. ifmo.ru/ru/university_live/achievements/news/6802/
24. https://vk.com/ video-129090933_456239022?api_access_key=585f3ac8e3e68c4647
25. «Российские хакеры — „лучшие в мире"», elérhető: https://www.securitylab.ru/news/215244.php
26. https://www.facebook.com/maxim.perlin/posts/745204182281015
27. «Лицом к лицу с хакером», elérhető: https://www.vedomosti. ru/newspaper/articles/2004/11/02/licom-k-licu-s-hakerom
28. «Планета CC. Золотое время Carderplanet», elérhető: https://bugtraq.ru/library/underground/planetacc.html
29. Uo.
30. «Планета хакеров: как создавался крупнейший в мире форум киберпреступников», elérhető: http://www. forbes.ru/tekhnologii/tekhnika-i-biznes/332679-planeta-khakerov-kak-sozdavalsya-krupneishii-v-mire-forum-kiber
31. «Кардинг. Интервью со Script'ом», elérhető: http://xakep-archive.ru/xa/039/048/3.html
32. «„Если бы не стукач, нас бы не нашли". История белорусского киберпреступника, живущего в США», elérhető: http://belgid.by/news/it/31784
33. https://www.kommersant.ru/ doc/639299
34. «Банковские карты легли удачно», elérhető: https://www.kommersant.ru/ doc/639299
35. Shadowy Russian Firm Seen as Conduit for Cybercrime, elérhető: http://www. washingtonpost.com/wp-dyn/



content/article/2007/10/12/ AR2007101202461_pf.html?noredirect=on
36. «Система координат», elérhető: https://www.romanvega.ru/p/intro.html
37. «Эксклюзивное интервью бывшего хакера, отсидевшего за киберворовство в США», elérhető: https://www.youtube.com/watch?v=3VIbPSPN8jE
38. «Система координат», elérhető: https://www.romanvega.ru/p/intro.html
39. «Как кардер вышел из тюрьмы и делает бизнес на кибербезопасности», elérhető: https://secretmag.ru/trends/players/naskovets-hacker.htm
40. https://docs.google.com/file/d/0ByQf4BUGl49wSVV0Uk45U3doS1U/edit
41. https://tgraph.io/Intervyu-s-izvestnym-karderom-08-10
42. Retail Hacking Ring Charged for Stealing and Distributing Credit and Debit Card Numbers from Major U.S. Retailers, elérhető: https://www.justice.gov/archive/opa/pr/2008/August/08-ag-689.html
43. https://carding.pro/ru/vodke-carder-i-hacker-byt/
44. «Планета хакеров: как создавался крупнейший в мире форум киберпреступников», elérhető: https://www.forbes.ru/ tekhnologii/tekhnika-i-biznes/332679-planeta-khakerov-kaksozdavalsya-krupneishii-v-mire-forum-kiber
45. «Как я украл миллион. Исповедь раскаявшегося кардера», Сергей Павлович (Питер, 2014)
46. BadB Welcome Cartoon, elérhető: https://www. youtube.com/watch?v=O_hP-Mrhv7U, https://www.youtube.com/watch?v=CEAMeVYqzSw
47. «Эксклюзивное интервью бывшего хакера, отсидевшего за киберворовство в США», elérhető: https://www.youtube.com/watch?v=3VIbPSPN8jE
48. https://www.nytimes.com/interactive/2017/04/21/technology/document-Seleznev-Letter. html?_r=0
49. Раненного в Марокко сына депутата везут в Москву для срочной операции», https://ria.ru/20110429/369552620.html
50. https://krebsonsecurity.com/wp-content/uploads/2014/07/Seleznev-Indictment-CR11-0070RAJ-1.pdf
51. Uo.

52. https://www.justice.gov/opa/press-release/file/904516/ download
53. «Хакер Роман Селезнев: взгляд из Москвы», elérhető: https://www.golos-ameriki.ru/a/vv-seleznev/1953487.htm
54. „Украинский след" в деле Селезнева», elérhető: https:// www.gazeta.ru/social/2014/08/09/6168613.shtml
55. Russian hacker called "Tony Soprano-style mob boss" is sentenced in Seattle to 27 years, elérhető: https://www. seattletimes.com/seattle-news/crime/prolific-russian-hacker-whoraked-in-millions-sentenced-to-27-years-in-prison/
56. Russian Cyber-Criminal Sentenced to 27 Years in Prison for Hacking and Credit Card Fraud Scheme, elérhető https:// www.justice.gov/opa/pr/ russian-cyber-criminal-sentenced-27-years-prison-hacking-andcredit-card-fraud-scheme
57. Russian Cyber-Criminal Pleads Guilty To Role In Organized Cybercrime Ring Responsible For $50 Million In Online Identity Theft, elérhető: https://www.justice.gov/usao-nv/ pr/russian-cyber-criminal-pleads-guilty-roleorganized-cybercrime-ring-responsible-50
58. «YouDo: с Porucheno.ru мы не конкуренты», elérhető https://roem.ru/25-03-2009/128464/youdo-sporuchenoru-my-ne-konkurenty/
59. «Одна звезда Владимира Кузьмина», elérhető: https:// www.mk.ru/culture/interview/2010/05/30/ 500105-odna-zvezda-vladimira-kuzmina-foto.html
60. «Владимир Кузьмин не признает родство с известным хакером», elérhető: https://www.vesti.ru/videos/show/ vid/681412/cid/1741/#/video/ https%3A%2F%2Fplayer .vgtrk.com%2Fiframe%2Fvideo%2Fid%2F1530869 %2Fstart _zoom%2Ftrue%2FshowZoomBtn%2Ffalse%2Fsid%2Fvesti %2FisP lay%2Ftrue%2F%3Facc_video_id%3D681412
61. «Первая жена Владимира Кузьмина: В смерти моих детей виновата Алла Пугачева!», elérhető: https://sobesednik.ru/ shou-biznes/ pervaya-zhena-vladimira-kuzmina-v-smerti-moikh-deteivinovata-alla-pugacheva
62. Nikita Kuzmin, Creator Of The Gozi Virus, Sentenced In Manhattan Federal Court, elérhető: https://www.justice. gov/usao-sdny/pr/nikitakuzmin-creator-gozi-virus-sentenced-manhattan-federal-court
63. US Sentences Proponent of «Hacker-for-Hire» Cybercrime,



elérhető https://www.voanews.com/a/us-sentences-proponent-of-hacker-for-hire-cybercrime/3312942.html
64. All the president's men's lawyers: who are Trumpworld's leading attorneys?, elérhető: https://www.theguardian. com/us-news/2017/jul/15/donaldtrump-russia-lawyers-kasowitz-futerfas
65. «Сын Трампа встречался с „адвокатом из Кремля" ради компромата на Хиллари Клинтон. При посредничестве певца Эмина Агаларова», elérhető: https://meduza.io /feature/2017/07/11/syn-donalda-trampa -vstrechalsya-sadvokatom-kremlya-radi-kompromata -na-hillari-klinton-priposrednichestve-pevtsa-emina-agalarova
66. https://roem.ru/29-02-2016/220224/bank-fns-tranborder/#comment-219896
67. Nikita Kuzmin, Creator Of The Gozi Virus, Sentenced In Manhattan Federal Court, elérhető: https://www.justice. gov/usao-sdny/pr/nikitakuzmin-creator-gozi-virus-sentenced-manhattan-federal-court
68. https://www.facebook.com/nikita.kouzmin
69. http://forum.navi.gg/counter-strike_obschiy/v_ moscow_ five_poyavilsya_kurator_proekta/
70. «„Империя" Матвиенко: чем владеет сын губернатора Петербурга», elérhető: https://www.dp.ru/a/2009/12/08/ Imperija_Matvienko_ chem
71. https://vk.com/wall130960779_290
72. https://vk.com/ wall130960779_279
73. https://vk.com/ddd1ms?w=wall130960779_368
74. Biggest U.S. Hack Case Is Tale of Gamers' Interrupted Vacation, доступно на https://www.bloomberg.com/ news/ articles/2015-01-12/biggest-u-s-hack-case-is-tale-ofgamers-interrupted-vacation
75. Russian National Admits Role in Largest Known Data Breach Conspiracy Ever Prosecuted, elérhető: https://www. justice.gov/opa/pr/ russian-national-admits-role-largest-known-data-breachconspiracy-ever-prosecuted
76. https://cyber.sports.ru/tribuna/ blogs/ explosivesheep/834007.html
77. https://vk.com/vipsmi?w=wall222255116_14
78. Biggest U.S. Hack Case Is Tale of Gamers' Interrupted Vacation, elérhető: https://www. bloomberg.com/news/

articles/2015-01-12/biggest-u-s-hack-case-is-tale-of-gamers-interrupted-vacation
79. «Белорусский „хакер", осуждённый в США: „Меня арестовывали 40 человек — Интерпол, ФБР, полиция"», elérhető: https://dev.by/news/belorusskiy-haker-osuzhdyonnyy-v-sshamenya-arestovyvali-40-chelovek-interpol-fbr-cheshskaya-politsiya
80. «Сбербанк оценил потери экономики РФ от кибератак за год в 600 млрд. рублей», elérhető: http://www.interfax.ru/business/512912
81. https://www.cbr.ru/StaticHtml/File/14435/FinCERT_survey.pdf
82. «Охота на Lurk», elérhető: https://securelist.ru/the-huntfor-lurk/2922
83. «Задержание хакеров», elérhető: https://www.youtube.com/watch?time_ continue=286&v=JOTldBImntw
84. «Штаб-квартира хакеров, похитивших более 1,7 миллиардов рублей у банков, была в Екатеринбурге», elérhető: https://www.ural.kp.ru/daily/26537.4/3553523/
85. «Троянцу подобрали команду», elérhető: https://www.kommersant.ru/doc/3292947
86. Uo.
87. «Антон Носик: Откуда в России хакеры?», elérhető: https://snob.ru/ selected/entry/13263
88. «Проверка интернет легенд -- Тихий дом», elérhető: https://www.youtube.com/watch?v=TFtuOdvy_is
89. https://netstalking.fandom.com/ru/wiki/ Тихий_дом
90. «Основатель Freedom Hosting арестован в Ирландии и ждет экстрадиции в США» elérhető: https://habrahabr.ru/post/188914/
91. FBI Admits It Controlled Tor Servers Behind Mass Malware Attack, elérhető: https://www.wired.com/2013/09/freedom-hosting-fbi/
92. Uo.
93. «Кремль и хакеры», elérhető: https://agentura. livejournal.com/51685.html
94. *...leveleket küldött szét:* Is Waledac Spam Dirtying the Russian 2012 Elections?, elérhető: https://www.symantec.com/connect/ru/blogs/waledac-spam-dirtying-russian-2012-elections?page=1
95. https://forum.antichat.ru/threads/vebmajl-rassylki-ot-severa.294101/



96. https://forum.antichat.ru/members/162854/
97. Arrested Russian's wife denies U.S. charge he is global hacking mastermind, доступно на https://uk.reuters.com/article/us-usa-cyber-botnet-wife/arrested-russians-wife-denies-u-s-chargehe-is-global-hacking-mastermind-idUKKBN1AA17U
98. «„Хватают исподтишка»: в МИД прокомментировали задержание российского программиста в Испании», elérhető https://www.ntv.ru/video/1381208/
99. «Программист Левашов заочно арестован», elérhető: https://iz.ru/661226/2017-10-20/programmist-levashovzaochno-arestovan-v-rossii
100. http:// phrack.org/issues/27/12.html
101. The Impact of Federal German Intelligence Service Bundesnachrichtendienst (BND) Project RAHAB and Chaos Computing Congresses (CCC) impact on the Future of Computer-Network Mediated Espionage: Cuckoo's Egg Prequel or Perfect Storm?, elérhető: https://www.afcea.org/committees/ cyber/documents/impactofbndprojectrahabandcccon thefutureofcomputer-networkmediatedespionage-cuckooseggpreque.pdf
102. W. German «Hackers» Tricked KGB, Paper Says, elérhető: http://articles.latimes. com/1989-03-06/news/mn-130_1_west-german
103. https://www.washingtonpost.com/archive/politics/1989/03/03/german-computer-hackers-held-forspying-for-soviets/b2fccb53-4939-48d8-b74e-30d3dcda88cb/?utm_ term=.c9b3e718065f
104. http://phrack. org/issues/25/10.html
105. Hans Heinrich Hübner; Ex Member of Chaos Computer Club (CCC), elérhető: http://paolodelbene.pbworks.com/w/page/50465475/ Hans%20Heinrich%20Hübner%3B%20Ex%20Member%20of%20Chaos%20Computer%20Club%20(CCC)
106. https://www.godlikeproductions.com/forum1/message993360/pg1?disclaimer=1
107. http://kremlin.ru/events/president/news/52830
108. https://primerussia. ru/article_materials/327.html
109. «С Лермонтовым наперевес», elérhető: https://www.kommersant.ru/doc/15879
110. «Томские хакеры 3 года ведут информационную войну

против чеченских экстремистов», elérhető: https://www.newsru.com/russia/30Jan2002/hakery.html
111. «Как Россия боролась с „Кавказ-центром"», elérhető: https://www.gazeta.ru/2006/03/09/oa_191473.shtml
112. «Не играйте за рулем», elérhető: http://www.itogi.ru/archive/2002/19/97277.html
113. «Пропагандистские ресурсы чеченских сепаратистов подверглись анонимной экзекуции», elérhető: http://www. membrana.ru/particle/13580
114. «ФСБ не видит нарушения закона в действиях томских хакеров против сайта „Кавказ-центр"», elérhető: https://www.newsru.com/russia/04feb2002/tomsk.html
115. https://web.archive.org/web/20060323114250/http://www.cyberantiterror.com:80/targets/
116. «Политподключенные», elérhető: https://www.kommersant.ru/doc/620317
117. https://web.archive.org/web/20051025000535/http://www.peace4peace.com:80/
118. «В Нальчик пришла война», elérhető: https://lenta.ru/articles/2005/10/13/nalchik/
119. «Wikileaks: Эстония отделалась легко», elérhető: https://inosmi.ru/baltic/20101211/164825182.html.
120. Denial-of-Service: The Estonian Cyberwar and Its Implications for U.S. National Security, elérhető: http://www.iar-gwu.org/ node/65
121. «Акция хакерского неповиновения», elérhető: https://www.kommersant.ru/ doc/1136738
122. Kremlin Kids: We Launched the Estonian Cyber War, elérhető: https://www.wired.com/2009/03/pro-kremlin-gro/
123. https://www.justice.gov/opa/press-release/file/956511/download
124. «Кибер-сюрприз», elérhető: https://www. novayagazeta.ru/articles/2007/05/31/33284-kiber-syurpriz
125. «Красиво жить не запретишь», elérhető: http://xakep-archive. ru/xa/093/086/1.htm
126. *Inside Cyber Warfare: Mapping the Cyber Underworld*, Jeffrey Carr (O'Reilly Media, 2011)
127. https://web.archive.org/ web/20080812013618/http://www.stopgeorgia.ru/
128. https://web.archive.org/web/20080812084132/http://www.stopgeorgia.ru/?pg=tar



129. «Сайты заняли оборону», elérhető: https://www.kommersant.ru/ doc/1010863
130. *Inside Cyber Warfare: Mapping the Cyber Underworld*, Jeffrey Carr (O'Reilly Media, 2011)
131. «Самые информированные люди в ГРУ», elérhető: http://nvo.ng.ru/forces/2012-10-12/11_gru.html
132. »Указ Президента Российской Федерации от 21 января 2011 года N74 «О составе научного совета при Совете Безопасности Российской Федерации», elérhető: https://rg.ru/2011/01/23/ sovbez-site-dok.html
133. «„Дождь" опубликовал обращение арестованного за госизмену сотрудника „Лаборатории Касперского"», доступно на https://meduza.io/ news/2017/04/12/dozhd-opublikoval-obraschenie-arestovannogoza-gosizmenu-sotrudnika-laboratorii-kasperskogo
134. «Соответствующий документ из Главного следственного управления МВД РФ по Санкт-Петербургу пришел в отдел расследований „Новой газеты", elérhető: https://www.novayagazeta. ru/news/2014/01/31/94678-po-mestu-prozhivaniya-spikera-171-homyachkov-187-bolonkina-vzyavshego-na-sebya-otvetstvennost-za-ddos-ataki-na-sayty-smi-v-aprele-mae-2013-budetvozbuzhdeno-ugolovnoe-delo
135. «За 7 млн рублей ИА „Мир" будет нести позитив в массы», elérhető: http://sanktpeterburg.bezformata.com/listnews/mir-budetnesti-pozitiv/26016420/
136. http://torquemada.bloground.ru/?p=1305
137. «МВД: почту Навального взломали с немецкого IP-адреса», elérhető: https://www.vedomosti.ru/politics/news/2012/08/29/mvd:pochtu-navalnogo-vzlomali-s-nemeckogo-ip-adresa
138. «Что за Хэлл? В Бонне начался суд по делу о взломе российских блогов: репортаж „Медузы»», elérhető: https://meduza.io/ feature/2015/06/24/chto-za-hell
139. https://www.crowdstrike.com/wpcontent/brochures/FancyBearTracksUkrainianArtillery.pdf
140. Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid, elérhető: https://www.wired.com/2016/03/inside-cunning-unprecedentedhack-ukraines-power-grid/?mbid=nl_3316
141. «Министр обороны РФ наградил солдат часами за

Дебальце-во», elérhető: https://citeam.org/putin-shoygu-debaltseve/
142. «Итоги международного расследования: „Боинг" сбили из российского „Бука"», elérhető: https://meduza.io/feature/2016/09/28/boing-sbili-izrossiyskogo-buka-glavnoe
143. https:// news-front.info/2016/02/24/kiberberkut-vzlomal-elektronnyeresursy-ruslana-levieva-18/
144. ThreatConnect reviews activity targeting Bellingcat, a key contributor in the MH17 investigation, доступно на https://threatconnect.com/ russia-hacks-bellingcat-mh17-investigation/
145. Pawn Storm Targets MH17 Investigation Team, elérhető: https://blog.trendmicro.com/trendlabssecurity-intelligence/pawn-storm-targets-mh17-investigation-team/
146. «Парень из нашего города, или „Как это бывает"», elérhető: http://xakep-archive.ru/xa/038/040/1.html
147. Russian Espionage Piggybacks on a Cybercriminal's Hacking, elérhető: https://www.nytimes.com/2017/03/12/world/europe/russia-hacker-evgeniy-bogachev.html?_r=0
148. How To Catch A Hacker, elérhető: https://www.buzzfeednews.com/article/sheerafrenkel/inside-the-hunt-for-russias-hackers
149. «Белгородец, осуществивший хакерскую атаку на официальный сайт ФСБ, выплатит судебный штраф в размере 40 тысяч рублей», доступно на http://oktiabrsky.blg.sudrf.ru/modules.php?name=press_dep&op=1&did=835
150. http://ens.mil.ru/files/morf/ Strategy.doc
151. «Ценность науки в предвидении», elérhető: https://www.vpk-news.ru/ articles/14632.
152. «Российскую „фабрику троллей" обвинили в разжигании споров о вреде прививок», elérhető: https://meduza. io/feature/2018/08/24/rossiyskuyu-fabriku-trolley-obvinili-vrazzhiganii-sporov-o-vrede-privivok
153. The Agency, elérhető: https://www.nytimes.com/2015/06/07/magazine/theagency-russian.html
154. https://intelligence.house.gov/uploadedfiles/6053177352305.pdf
155. U.S. Cyber Command operation disrupted Internet access of Russian troll factory on day of 2018 midterms, elérhető: https://www.washingtonpost.com/world/ national-security/us-cyber-command-operation-disruptedinternet-access-of-russian-troll-factory-on-day-of-2018-midterms/2019/02/26/1827fc9e-36d6-11e9-af5b-b51b7ff32-2e9_story. html?noredirect=on&utm_term=.80619f6afbcd
156. «Сергей Шойгу объявил о „большой охоте" на молодых программистов», elérhető: http://www.cnews.ru/news/top/sergej_shojgu_obyavil_o_ bolshoj_ohote
157. «В российской армии может появиться киберкомандование, заявил Рогозин», elérhető: https://ria. ru/20120321/601798789.html
158. «Шойгу сравнил угрозу кибербезопасности с оружием массового поражения», elérhető: https://ria.ru/20131019/971215505.html
159. «Владимир Путин: Нужно усилить защиту государства от информационных атак», elérhető: https://tass.ru/politika/629732
160. «Источник в Минобороны: в Вооруженных Силах РФ созданы войска информационных операций», elérhető https://tass.ru/ politika/1179830
161. «В России созданы кибервойска», elérhető: https://www.vesti.ru/doc.html?id=1573024
162. https://vk.com/ doc-94744292_437246143
163. https://www. nstu.ru/education/army_research
164. http://itschool.mil.ru
165. «Солдаты научной роты Военной академии связи подписали первый контракт с Минобороны», elérhető: https://function.mil.ru/news_page/country/more.htm?id=12071767@egNews
166. https://recrut.mil.ru/ for_recruits/research_company/companies/7NRvas.htm
167. «Рядовой хакер», elérhető: https://rg.ru/2013/07/10/roty-site.html?utm_source=rg. ru&utm_medium=offline&utm_campaign=back_to_online
168. *Kremlin's ties to Russian cyber gangs sow US concerns*, elérhető: https://thehill.com/policy/cybersecurity/256573kremlins-ties-russian-cyber-gangs-sow-us-concerns
169. «*Я – русский оккупант*»: https://www.youtube.com/watch?v=FYy1ivz7jXQ
170. http://fancybear.net
171. http://army-today.ru/karera-i-obrazovanie/ devyataya-nauchnaya/
172. elérhető: https://recrut.mil.ru/for_recruits/research_company/ companies/6NR_KVVU.htm

173. http://www.ulstu.ru/main?cmd=file&object=14214
174. «Заместитель министра обороны генерал-полковник Юрий Садовенко открыл новый учебный год в Рязанском высшем воздушно-десантном командном училище», elérhető: https://function.mil.ru/news_page/country/more.htm?id=11981620@egNews
175. «В ходе СОУ „Щит Союза-2015» связисты ЗВО отразили кибератаку условного противника», elérhető: https://function.mil.ru/news_page/country/more.htm?id=12056193@egNews
176. «Капицы в погонах: один день из жизни научной роты ВКО», elérhető: https://tvzvezda.ru/ news/forces/content/201411252109-vug9.htm
177. «В бой идут одни программисты», elérhető: http://army-today. ru/karera-i-obrazovanie/v-boy-idut-programmisty/?sphrase_ id=703503
178. «Китов Анатолий Иванович — пионер кибернетики, информатики и автоматизированных систем управления», В. А. Долгов (КОС•ИНФ, 2010)
179. «Кибернетика — „наука" мракобесов?», elérhető: https://www.kp.ru/ daily/22526/16560/
180. «Китов Анатолий Иванович — пионер кибернетики, информатики и автоматизированных систем управления», В. А. Долгов (КОС•ИНФ, 2010)
181. Uo.
182. «Интернет полковника Китова», elérhető: https://tvkultura.ru/brand/show/brand_id/59074
183. https://www.nsa.gov/Portals/70/ documents/resources/everyone/digital-media-center/videoaudio/historical-audio/nsa-60th/nsa-60th-1960s/19600701_MitchellandMartin.pdf
184. https://www.washingtonpost.com/opinions/nsa-secrets-revealed-in-1960/2013/06/21/35e0f072-d509-11e2-a73e-826d299ff459_story. html?utm_term=.122c9ba3b428
185. «От „Ультры" — до „Эшелона"», elérhető: https://chesspro.ru/_events/2009/neistadt.html
186. http://documents.theblackvault.com/documents/nsa/75791A.pdf
187. http://ens.mil.ru/science/SRI/infrmation. htm?id=12014@morfOrgScience
188. https://www.rdi-kvant.ru/Branches.aspx/
189. http://docs.cntd. ru/document/902053316



190. https://wikileaks.org/hackingteam/emails/emailid/587613
191. http://www.hackingteam.it
192. https://www.wikileaks.org/ hackingteam/emails/emailid/576384
193. https://ht.transparencytoolkit.org/Amministrazione/01%20-%20CLIENTI/5%20-%20Analisi%20Fatturato/2015/02%20-%20Client%20Overview%202015/Client%20 Overview_list_20150131.xlsx
194. «Российский заказчик Hacking Team подтвердил приобретение шпионского ПО», elérhető: https://www.forbes.ru/news/293525-rossiiskii-zakazchikhacking-team-podtverdil-priobretenie-shpionskogo-po
195. https://web.archive.org/web/20160504133551/http://mts-slil.info/
196. „Страна больна, если шпионов ищут среди кухарок и матерей". Как живет семья Светланы Давыдовой, которую обвиняют в госизмене», elérhető: https://meduza.io/ feature/2015/01/30/strana-bolna-esli-shpionov-ischut-sredi-kuharok-i-materey
197. «Научно-исследовательский институт ФСБ проводил нелегальные закупки в США», elérhető: https://www.securitylab.ru/ news/442272.php
198. «Опыт выявления уязвимостей в зарубежных программных продуктах», elérhető: https://s3r.ru/wp-content/uploads/2013/12/ Kiber_Bezop_—1_2013_42.pdf
199. https://twitter.com/BivolBg/status/860803144103723009
200. «В метаданных взломанных писем Макрона обнаружилось имя русского хакера», elérhető: https://theins.ru/politika/55118
201. «Рошка и мышка. Почту президента Франции взломали сотрудники ГРУ», elérhető: https://theins.ru/politika/58803
202. «Нидерланды обвинили четверых россиян в хакерской атаке. Подтвердить их связь с ГРУ может почти каждый», elérhető: https://meduza.io/slides/niderlandyobvinili-chetveryh-rossiyan-v-hakerskoy-atake-podtverdit-ihsvyaz-s-gru-mozhet-pochti-kazhdyy
203. «Козачек, он же Kazak, он же blablabla1234565», elérhető: https://meduza. io/feature/2018/07/13/kozachek-on-zhe-kazak-on-zheblablabla1234565
204. https://mikhailmasl.livejournal.com/5591.html
205. «О подготовке кадров в области информационной

безопасности», elérhető: http://emag.iis.ru/arc/infosoc/emag. nsf/BPA/2bc575e2571effc8c32575bd00428b4e
206. https://multiurok.ru/blog/proforiientatsionnaia-rabota-po-podghotovkie-budushchikhspietsialistov-v-oblasti-informatsionnykh-tiekhnologhii-dliasilovykh-struktur-i-voienno-patriotichieskogho-vospitaniiamolodiezhi.html
207. «Подведение итогов, презентация проекта ЦМВС МО РФ», elérhető: https://www.youtube.com/watch?v=wziNiqKpuiY
208. https://www.slideshare.net/sergheiepifantsew5/ctf-72571006 (a prezentációt eltávolították)
209. http://www.1770.ru/date-news/2016-12 (Страница недоступна — когда о деятельности «Юных программистов ФСБ» рассказала «Медуза», они удалили со своих сайтов и соцсетей почти все материалы)
210. https://vk.com/ album-83710188_238873694
211. http://www.1770.ru/datenews/2016-12 (az oldalt eltávolították)
212. https://lydidela.files.wordpress.com/2016/08/ bn_wd3eijrc.jpg?w=570&h=380
213. https://hghltd.yandex.net/yandbtm?fmode=inject&url=https%3A%2F%2Fwww.slideshare.net%2FTCenter500%2F1770-50748329&tld=ru&lang=en&la=1494592128&tm=1495190464&text=проект юные программисты фсб россии&l10n=ru&mime=html&sign=e74453762663bde3f3188ae1c51ee5e3&keyno=0 (az oldalt eltávolították)
214. https://www.youtube.com/watch?v=s7SBGSDpRCk&feature=youtu.be (a videót eltávolították)
215. http://www.dslib.net/kult-prosvet/formirovanie-motivacii-k-voennoj-sluzhbe-u-junoshej-doprizyvnogo-vozrasta-v-processe.html
216. https://vk.com/ album-83710188_237553428
217. https://www.instagram. com/p/9bDNyIhYvK/
218. https://vk.com/ludydela?z=photo83710188_377623796%2Falbum-83710188_208871221%2Frev (фотография удалена)
219. «Шкворень: школьники переводят книгу про хакеров», elérhető: https://habr.com/ru/post/261491/
220. https://fsb.ru.com/%20наши-достижения/ (az oldalt eltávolították)



221. https://multiurok.ru/blog/naghrazhdieniie-znakom-fsb-rf.html (az oldal azóta nem található)
222. https://www.youtube.com/ watch?v=eYPPRKKKvp4 (a videót eltávolították)
223. https://www.instagram.com/p/BTOlMNFgbga/?taken-by=itcoder (a posztot eltávolították)
224. https://www.youtube.com/ watch?v=26zTC8eDmzE (a videót eltávolították)
225. «Дети боевого братства», elérhető: https://www.youtube.com/watch?v=cBrr9kcnQY0
226. https://sch1770.mskobr.ru/common_edu/moskovskij_kadetskij_muzykal_nyj_korpus/obwie_svedeniya/pedagogicheskij_kollektiv/uchitelya_matematiki_i_informatiki/epifancev_sergej_ vladimirovich/
227. *Dark Territory: The Secret History of Cyber War*, Fred Kaplan (Simon & Schuster, 2017)
228. We're In The Middle Of A Cyerwar, elérhető: https://www.newsweek.com/were-middle-cyerwar-166196
229. Commentary: Don't be so sure Russia hacked the Clinton emails, elérhető: https://www.reuters.com/article/us-russiacyberwar-commentary-idUSKBN12X075
230. «Песков: Россия не причастна к атаке хакеров на американские базы данных», elérhető: https://www.vesti.ru/doc. html?id=2765084
231. Background to «Assessing Russian Activities and Intentions in Recent US Elections»: The Analytic Process and Cyber Incident Attribution, elérhető: https://www.dni.gov/ files/documents/ICA_2017_01.pdf
232. https://www.welivesecurity.com/wp-content/uploads/2016/10/eset-sednit-part1.pdf
233. «Хакеры атаковали ВАДА», elérhető: https://meduza.io/feature/2016/09/13/hakeryatakovali-vada
234. https://www.welivesecurity.com/wp-content/uploads/2016/10/eset-sednit-part1.pdf
235. A Voice Cuts Through, and Adds to, the Intrigue of Russia's Cyberattacks, elérhető: https://www.nytimes.com/2016/09/28/world/europe/russia-hacker-vladimir-fomenko-king-servers. html?_r=0
236. «Холодная хакерская во-йна У Агентства национальной безопасности США, кажется, украли кибероружие», elérhető: https://meduza.io/ feature/2016/08/17/holodnaya-hakerskaya-voyna

237. «Минобороны РФ ищет специалистов по реверс-инжинирингу», elérhető: https://news.softodrom.ru/ap/b19249.shtml
238. https://www.welivesecurity.com/wp-content/uploads/2016/10/eset-sednitpart1.pdf
239. The CozyDuke APT, elérhető: https://securelist.com/the-cozyduke-apt/69731/
240. The CozyDuke APT, elérhető: https://securelist.com/the-cozyduke-apt/69731/...*A bírósági dokumentumokban részletesen ki volt fejtve:* https://www.justice.gov/file/1080281/download
241. «В США предъявили обвинения 12 сотрудникам ГРУ по делу о вмешательстве в выборы», elérhető: https://meduza.io/news/2018/07/13/v-ssha-pred-yavili-obvineniya-12-sotrudnikam-gru-po-delu-o-vmeshatelstve-vvybory
242. «11 часов допроса», elérhető: https://meduza.io/feature/2015/10/23/11-chasov-doprosa
243. Top Russian Cybercrimes Agent Arrested on Charges of Treason, elérhető: https://www.nytimes.com/2017/01/25/world/europe/sergeimikhailov-russian-cybercrimes-agent-arrested.html
244. «Образцово-показательное унижение», elérhető: https://lenta.ru/articles/2013/07/05/kamenskuralsky/
245. https://www.vedomosti.ru/newspaper/articles/2004/11/02/licom-k-licu-s-hakerom
246. https://web.archive.org/web/20050410043421/http://kamensk.net.ru:80/forb/info/common/my.html
247. «История журнальных компьютерных хулиганов», elérhető: https://xakep.ru/2007/12/04/x-history-1999-2007/
248. https://soundcloud.com/5qlw9z0f2kxa/15-08-2017
249. «Взломанный твиттер РИА Новости сообщил о смерти Горбачева», elérhető: https://lenta.ru/news/2013/08/08/ria/
250. IAEA chief: Nuclear power plant was disrupted by cyber attack, elérhető: https://uk.reuters.com/article/us-nuclear-cyberidUKKCN12A1OC
251. «Организационно-технические проблемы защиты от целевых вредоносных программ типа STUXNET», elérhető: https://s3r.ru/wp-content/uploads/2013/12/Kiber_Bezop_—-1_2013_28.pdf
252. «ФСБ выявила вирус для кибер-шпионажа в сетях 20



госорганов и предприятий ОПК», доступно на https://tass.ru/ekonomika/3498890
253. «За чиновниками шпионили через web-камеры», elérhető: https://www.gazeta. ru/tech/2016/07/30_a_9720437.shtml
254. Uo.
255. «Эксперты обнаружили атаку хакеров на военно-промышленный комплекс России», elérhető: https://www.rbc.ru/technology_ and_media/08/02/2018/5a7c3ee29a79471c93ab30b3
256. http://www.tadviser.ru/index.php/Статья:Единая_сеть_пе-редачи_данных_(ЕСПД)_для_госорганов_(Russian_State_Network,_ RSNet)
257. http://stcnet.ru/products_iid_17.htm
258. «Internet тотального контроля», elérhető: https://www.kommersant.ru/doc/14591
259. «Вызовы в сфере информационной безопасности: оценка актуальности угроз», elérhető: http://studies.agentura.ru/listing/vyzovi/
260. http://xakep-archive.ru/xa/046/050/1.htm
261. Obama Order Sped Up Wave of Cyberattacks Against Iran, elérhető: http://www.nytimes.com/2012/06/01/world/middleeast/obamaordered-wave-of-cyberattacks-against-iran.html
262. http://www.zerodaysfilm.com/
263. An Unprecedented Look at Stuxnet, the World's First Digital Weapon, elérhető: https://www.wired.com/2014/11/countdownto-zero-day-stuxnet/
264. Obama's secret struggle to punish Russia for Putin's election assault, elérhető: https://www.washingtonpost.com/graphics/2017/world/national-security/obama-putinelection-hacking/?pushid=594cf6ea2e12651d00000094&tid=not ifi_push_breaking-news&utm_term=.cff22297a4f4
265. http://www.zerodaysfilm.com
266. «Вызовы в сфере информационной безопасности: оценка актуальности угроз», elérhető: http://studies.agentura.ru/listing/vyzovi/
267. Inside the hacker underworld of ISIS, elérhető: https://www.businessinsider. com/isis-hacking-division-operates-2016-6
268. Uo.
269. The Curious Case of the Jihadist Who Started Out as

a Hacktivist, elérhető: https://www. vanityfair.com/news/2015/12/isis-hacker-junaid-hussain
270. ExTeaMp0isoN Leader «TRiCk» Linked to Hackers Taking Over @CENTCOM, elérhető: https://news.softpedia.com/news/Ex-TeaMp0isoN-Leader-Trick-Linked-to-Hackers-Taking-OverCENTCOM-470094.shtml
271. British hacker is No 3 on Pentagon «kill list», elérhető: https://www.thetimes.co.uk/article/british-hacker-is-no-3on-pentagon-kill-list-6g95bfqwfnz
272. https://imgur.com/b1t98pl
273. Hacker Outs Himself as FBI «Snitch» and Claims He Helped Track Down ISIS, elérhető: https://motherboard.vice.com/en_us/article/nz7w9b/hackerouts-himself-as-fbi-snitch-and-claims-he-helped-track-downisis
274. https://www.group-ib.ru/resources/threat-research/2016-report. html
275. The Doomsday Scam, elérhető: https://www.nytimes.com/2015/11/22/magazine/the-doomsday-scam.html
276. Указ Президента Российской Федерации от 15 января 2013 г. N31c г. Москва «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации», elérhető: https:// rg.ru/2013/01/18/komp-ataki-site-dok.html
277. http://www.fsb.ru/ files/PDF/Vipiska_iz_koncepcii.pdf
278. "Ростех" занялся парированием киберугроз», elérhető: https://iz.ru/news/642771
279. «BIS TV — НКЦКИ: Состояние и перспективы развития (Алексей Новиков) — IX Уральский форум», elérhető: https://www.youtube.com/watch?v=c7gOPOFBQX0
280. http://asozd.duma.gov.ru/addwork/scans.nsf /ID/EBE024490F4C5851432580810054D3AC/$File /47571-7_06122016_47571-7.PDF? OpenElement
281. «Владимир Путин выступил на коллегии ФСБ», elérhető: https://www.1tv.ru/news/2015-03-29/22210-vladimir_putin_ vystupil_na_kollegii_fsb
282. http://www.video.duma.gov.ru/watch/?id=310933
283. http://asozd2.duma.gov.ru/main.nsf/(SpravkaNew)? OpenAgent&RN=47571-7&02
284. «Глава ФСБ попросил Думу ускорить принятие законов о регулировании в Сети», elérhető: https://www.rbc.ru/politics/23/06/2017/594 ceb609a7947265009bfc8



285. «Информационной инфраструктуре придали критическую скорость», elérhető: https://www.kommersant.ru/doc/3344780
286. «Российские власти хотят изолировать интернет. Теперь у нас будет как в Китае?», elérhető: https://meduza.io/feature/2018/12/17/rossiyskievlasti-hotyat-izolirovat-internet-teper-u-nas-budet-kak-v-kitae
287. https://www.ptsecurity.com/ ru-ru/products/isim/, https://www.group-ib.ru/tds.html, https://media .kaspersky.com/pdf/Kaspersky_Industrial_ CyberSecurity _brochure.pdf
288. «Посторонних нет: как создавался бизнес по охране государственных секретов», elérhető: http://www.forbes.ru/kompanii/internet-telekomi-media/314311-postoronnikh-net-kak-sozdavalsya-biznes-pookhrane-gosudars
289. https://www.securitycode.ru/company/news/kompaniya_informzashchita_poluchila_novyy_sertifikat_fsb_rossii_na_apksh_kontinent/
290. «Еще одна маленькая девочка-хакер», elérhető: https://meduza.io/ feature/2016/12/30/esche-odna-milenkaya-devochka-haker
291. https://www.instagram.com/ alisaesage/?hl=ru
292. «Еще одна маленькая девочка-хакер», elérhető: https://meduza. io/feature/2016/12/30/esche-odna-milenkaya-devochka-haker
293. «Контракт со взломом: как хакер построила бизнес за счет банков и корпораций», elérhető: https://www.forbes.ru/tekhnologii/internet-i-svyaz/275355kontrakt-na-ugrozu-kak-khaker-stroit-biznes-na-zashchitebankov
294. FACT SHEET: Actions in Response to Russian Malicious Cyber Activity and Harassment, elérhető: https://obamawhitehouse.archives.gov/the-pressoffice/2016/12/29/fact-sheet-actions-response-russian-malicious-cyber-activity-and
295. http://zorsecurity.ru
296. «Холодная хакерская война», elérhető: https://meduza.io/feature/2016/08/17/holodnaya-hakerskaya-voyna
297. The need for urgent collective action to keep people safe online: Lessons from last week's cyberattack, elérhető: https://blogs.microsoft.com/on-the-issues/2017/05/14/need-urgent-collective-action-keeppeople-safe-online-lessons-last-weeks-cyberattack/

298. He Perfected a Password-Hacking Tool — Then the Russians Came Calling, elérhető: https://www.wired.com/story/how-mimikatz-became-go-to-hacker-tool/
299. White House blames Russia for «reckles» NotPetya cyber attack, elérhető: https://ca.reuters.com/article/technologyNews/ idCAKCN1FZ2UJ-OCATC
300. «Угрозы информационной безопасности становятся все более изощренными и масштабными», elérhető: https://www.kommersant.ru/ doc/3303788
301. https://www.group-ib.ru/blog/wannacryptor
302. Locating Mobile Phones using Signalling System #7, доступно на https://berlin.ccc.de/~tobias/25c3-locating-mobile-phones.pdf
303. Here's Why Anyone Could Hack Your Phone, elérhető: https://www.thedailybeast.com/heres-why-anyone-could-hackyour-phone
304. New documents show how the NSA infers relationships based on mobile location data, elérhető: https://www.washingtonpost.com/ news/the-switch/wp/2013/12/10/new-documents-show-how-the-nsainfers-relationships-based-on-mobile-location-data/?utm_term=.fbfee6aede3b
305. For sale: Systems that can secretly track where cellphone users go around the globe, elérhető: https://www.washingtonpost.com/business/technology/for-sale-systemsthat-can-secretly-track-where-cellphone-users-go-around-theglobe/2014/08/24/f0700e8a-f003-11e3-bf76-447a5df6411f_story. html?utm_term=.8ae6beff86b1
306. German researchers discover a flaw that could let anyone listen to your cell calls, elérhető: https://www.washingtonpost.com/news/the-switch/ wp/2014/12/18/german-researchers-discover-a-flaw-that-could-
307. «Атака хакеров: как пропадают миллиарды», elérhető: https://hbr-russia.ru/ biznes-i-obshchestvo/fenomeny/a16348/
308. «Как взломать Telegram и WhatsApp: спецслужбы не нужны», elérhető: https://habr.com/ru/company/pt/blog/283052/
309. Cell Phone Network Flaws Can Help Spies Get Around Encryption Apps, elérhető: https://motherboard.vice.com/en_us/article/78k4vb/cellphone-network-flaws-can-help-spies-get-around-encryption-apps



310. https://www2.fireeye.com/rs/fireye/images/rpt-m-trends-2015.pdf
311. https://soundcloud.com/ kozlovsky/mts-otb
312. «МТС опроверг „целенаправленное" отключение SMS оппозиционерам во время взлома Telegram», elérhető: https://meduza.io/news/2016/04/29/mts-oprovergtselenapravlennoe-otklyuchenie-sms-oppozitsioneram-vo-vremyavzloma-telegram
313. «Верховный суд поддержал прослушку оппозиционеров», elérhető: https://republic.ru/posts/l/864280
314. «Колпак для оппозиции: как советская система прослушки возродилась в России», elérhető: https://www.forbes.ru/tehno/ tehnologii/231333-kolpak-dlya-oppozitsii-kak-sovetskayasistema-proslushki-vozrodilas-v-rossii
315. https://lj.rossia.org/users/kremlingate/?skip=20
316. «Печатный станок: как Василий Якеменко создал финансовую пирамиду на книгах», elérhető: https://tvrain.ru/teleshow/bremja_novostej/ yakemenko-431316/
317. https://twitter.com/yakemenko/status/219393783568146432
318. «Боты — новые солдаты», elérhető: http://mag.afisha. ru/stories/realnosti-ne-sushestvuet/boty-novye-soldaty/
319. «Мы делаем то, что нам велит наша совесть», elérhető: https://daily.afisha.ru/archive/ gorod/archive/anonymous-russia/
320. «Взломщики почты Якеменко пригрозили разоблачениями „продажным блоггерам и чиновникам"», elérhető: https://www.newsru.com/russia/08feb2012/anon.html
321. «Хакер вне политики», elérhető: https://www.kommersant.ru/doc/2375565
322. «Обращение Anonymous к гражданам России», elérhető: https://www.youtube.com/watch?v=zGVnZShlZ1E
323. «Как устроен Роскомнадзор», elérhető: https://meduza.io/feature/2015/03/13/kak-ustroenroskomnadzor
324. http://asozd2.duma.gov.ru/main.nsf/(Spravka)?OpenAgent&RN=553424-6
325. «„Пакет Яровой"принят больше полугода назад. Как он работает?», elérhető: https://meduza.io/feature/2017/02/13/zakon-yarovoy-prinyatbolshe-polugoda-nazad-kak-on-rabotaet

326. «Основная мишень — пользователи», elérhető: https://meduza.io/feature/2018/02/05/osnovnaya-mishenpolzovateli
327. https://twitter.com/Russian_Revolt/status/444364017608720384
328. Anonymous Russia — Fancy Bears Operation Olympics, elérhető: https://www.youtube.com/watch?v=BSgxms6Lz_U
329. «Сотни троллей за миллионы», elérhető: https://www.fontanka. ru/2014/05/29/170/
330. http://b0ltay.blogspot.com/
331. «Аркадий Дворкович стал жертвой хакеров», elérhető: https://www.vedomosti.ru/politics/articles/2014/07/22/arkadij-dvorkovich-postupil-v-rassylku
332. https://www.rbc.ru/society/14/08/2014/570420ae9a794760d3d40b3f
333. «Хакеры опубликовали переписку СМИ о проплаченных предвыборных статьях», elérhető: https://www.novayagazeta.ru/news/2014/09/24/105893-hakeryopublikovali-perepisku-smi-o-proplachennyh-predvybornyh-statyah
334. https://meduza.io/news/2014/10/30/v-set-popalaperepiska-zamnachalnika-sekretariata-igorya-shuvalova
335. «Анонимный интернационал: „Потупчик получила в АП не менее 15 миллионов"», elérhető: https://theins.ru/politika/2230
336. «Письма Администрации президента: как заказали Навального», elérhető: https://theins.ru/politika/2349
337. «Неравнодушные люди сами виноваты, что потеряли интернет», elérhető: http://www.lookatme.ru/mag/people/manifesto/206757-shaltayboltay
338. «„Мы не маленькие дети в этом бизнесе": „Шалтай-Болтай" — о своих последних сливах», доступно на https://apparat.cc/world/ boltai/
339. https://web.archive.org/web/20141105174535/http://spektr.delfi. lv/novosti/my-ne-slivaem-my-rasskazyvaem-pravdu.d?id=45161768
340. «Сооснователь „Шалтая-Болтая" — Собчак: „ФСБ обещала гарантировать нам безопасность"», elérhető: https://tvrain.ru/teleshow/sobchak_zhivem/shaltai-427271/

# Tartalomjegyzék

Előszó ..... 7

I. RÉSZ. **GYÖKEREK** ..... 27
1. fejezet – A szabadság területe ..... 29
2. fejezet – Hogyan károsították meg Ászja nénit? ..... 34
3. fejezet – A kétségek félelemmé váltak ..... 40
4. fejezet – Diákok feltörik a NASA-t ..... 44
5. fejezet – Iskola a feltörők számára ..... 49
6. fejezet – A végzett növendék ..... 54

II. RÉSZ. **PÉNZ** ..... 59
7. fejezet – A hekkerek bolygója ..... 61
8. fejezet – A krími disszidens ..... 70
9. fejezet – A fehérorosz Ali Baba ..... 74
10. fejezet – A teslás kalandor ..... 79
11. fejezet – pSzih ..... 83
12. fejezet – A startupper ..... 92
13. fejezet – A sportember ..... 97
14. fejezet – Az ügyvéd ..... 101
15. fejezet – A rejtőzködők ..... 104
16. fejezet – A nyomozók ..... 108
17. fejezet – Feketepiac ..... 112
18. fejezet – Oroszország fő spammerje ..... 122

III. RÉSZ. **HATALOM** ..... 129
19. fejezet – A KGB-s medvebocs ..... 131
20. fejezet – Patrióta hekkerek ..... 137
21. fejezet – Megfékezni Grúziát ..... 144

22. fejezet – Hekkerek a liberálisok ellen ..... 149
23. fejezet – A világításnak befellegzett ..... 153
24. fejezet – Feltörők állami szolgálatban ..... 158
25. fejezet – Geraszimov doktrínája ..... 163
26. fejezet – A reakciósok tudománya ..... 172
27. fejezet – A „Kvantum" és a „Galilei" ..... 182
28. fejezet – A titkosítás katonái ..... 190
29. fejezet – Az FSZB ifjú programozói ..... 195

IV. RÉSZ. **HÁBORÚ** ..... 201
30. fejezet – A divatos medve ..... 203
31. fejezet – „Orkok" mint elvtársak ..... 213
32. fejezet – Őszinte vallomás ..... 219
33. fejezet – Az én számítógépes védelmem ..... 224
34. fejezet – Az összvilági zsaroló ..... 239
35. fejezet – Kémkednek utánunk ..... 244
36. fejezet – Az anonimek az állam ellen ..... 253
37. fejezet – A bangkoki összekötő ..... 264

Köszönetnyilvánítás ..... 284
Fogalomtár ..... 285
Végjegyzetek ..... 289

*A 2013-as moszkvai polgármester-választá*
*idején a Qrator védte Alekszej Navalnij*
*weboldalát; az ellenzéki politikus jelöltette*
*magát, és sikeres kampányt folytatott.*
*Vjarja egyszer észrevett egy lesötétített*
*ablakú furgont az irodájuk mellett,*
*a tetején antennákkal. A következő*
*napokban a furgon szinte mindennap*
*megjelent. Amikor kimentek ebédelni,*
*a Qrator munkatársai megpróbáltak*
*benézni a kocsiba, és azon tréfálkoztak,*
*hogy fánkot kéne hozni annak,*
*aki lehallgatja őket.*
*„– Szása tehetséges ember, de nagyon érzéke*
*és bogaras – mesélte Vjarja egykori főnöke,*
*Alekszandr Ljamin. – Ha túl sokáig*
*dolgozol az informatikai védelem területén*
*kezdesz megváltozni, kezdesz mindenben*
*fenyegetést látni."*

# DANYIIL TUROVSZKIJ

Újságíró, szerkesztő, tudósító. Moszkvában született 1990-ben. Pályafutása során olyan jelentős orosz internetes lapoknál dolgozott, mint a *Lenta.ru* vagy a *Meduza.io*. 2015-ben az Iszlám Államról írott cikksorozatát a brit *The Guardian* is átvette, s ezért a munkájáért az angol *GQ* magazin *Az év újságírója* díjjal tüntette ki.
Az orosz hekkerek történetéről szóló könyve Oroszországban 2019-ben jelent meg.

9 789635 430154

A moszkvai szerzőt, Danyiil Turovszkijt valaha szintén vonzotta a számítógépes kalózkodás, ám végül az egyik legnépszerűbb orosz internetes hírportál újságírója lett. Könyvében azoknak a szovjet gyerekeknek a történetét meséli el, akik kamaszkorukban az utolsó kopejkáikból vették meg a népszerű *Hekker* című magazint, felnőve pedig milliókat keresnek azzal, hogy weboldalakat törnek fel. Van köztük olyan, aki éppen sokéves börtönbüntetését tölti egy amerikai cellában, de olyan is, aki megmaradt etikus hekkernek, és nagyvállalatok számítógépes védelmi rendszerének kidolgozásában segít. Turovszkij könyve azt igyekszik megértetni velünk, hogy a számítógép és az okostelefon nem a barátunk – inkább a leggyengébb láncszemei személyes adataink védelmének.

Az orosz hekkerek történetét bemutató munkájában a szerző nemcsak az első orosz informatikai kalózok viselkedés-lélektanát, hanem a mai Oroszország kiberbűnözőinek és a velük szembeszállóknak a motivációit is tanulmányozza. Turovszkij könyvéből az is kiderül, vajon miért éppen a szabaddá váló kilencvenes években jelentek meg és váltak fogalommá az orosz hekkerek.

Csatlakozzon közösségünkhöz,
vegyen részt nyereményjátékainkban!
**www.facebook.com/athenaeumkiado**